



AEROSPACE RECOMMENDED PRACTICE

ARP5150™

REV. A

Issued 2003-11
Reaffirmed 2013-05
Revised 2019-01

Superseding ARP5150

(R) Safety Assessment of Transport Airplanes in Commercial Service

RATIONALE

Some information was not included in the first version that we now have material to include, plus some corrections and clarifications to existing text. The addition of sources of information publicly available on the internet was added. Also, all aviation companies need to include the Safety Management System process in their safety process and therefore some of that material needs to be added.

TABLE OF CONTENTS

1.	SCOPE	3
1.1	Purpose	3
1.2	How to Use This Document	3
1.3	Intended Users	4
2.	REFERENCE DOCUMENTS, DEFINITIONS, AND ACRONYMS	4
2.1	Applicable Documents	4
2.1.1	Airworthiness Documents	4
2.1.2	Industry Documents	5
2.1.3	Military Publications	5
2.2	Definitions	5
2.3	Acronyms	8
3.	SAFETY PROCESSES IN THE OPERATING FLEET	10
3.1	Overview of the Ongoing Safety Assessment Process	10
3.2	The Ongoing Safety Assessment Process	11
3.2.1	Establish Monitor Parameters	13
3.2.2	Monitor for Events	15
3.2.3	Assess Event and Risk	16
3.2.4	Develop Action Plan	20
3.2.5	Disposition Action Plan	22
3.2.6	Lessons Learned	23
3.3	The Integrated Ongoing Safety Assessment	24
3.4	Related Topics	26
3.4.1	Review of Process and Organization Effectiveness	26
3.4.2	Alternative Dispatch Conditions	26
3.4.3	Design Changes	26

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2019 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

**SAE values your input. To provide feedback
on this Technical Report, please visit
<http://standards.sae.org/ARP5150A>**

3.4.4	Alternative Parts	27
3.4.5	Safety Processes and Human Performance	28
3.4.6	Maintenance Program Development	28
3.4.7	Process to Appendix Cross Reference	29
4.	IN-SERVICE DATA	30
4.1	The Systemic View of Safety Information	30
4.2	Categories of Data	30
4.2.1	Accident Data	30
4.2.2	Incident Data	32
4.2.3	Safety Recommendation Data	32
4.2.4	Other Official Data	32
4.2.5	Data from Manufacturers	33
4.2.6	Operator-Level Data	33
5.	METHODS AND TOOLS	35
5.1	Root Cause (Event Tree) Analysis	35
5.2	Weibull Analysis	36
5.3	Monte Carlo Simulation Analysis	36
5.4	Corrective Action Scheduling	37
5.5	Sensitivity Analysis	37
5.6	Reliability Growth Modeling	37
5.7	Human Factors Methods and Tools	37
5.7.1	FOQA	38
5.7.2	MEDA Tool	38
5.8	Fleet Risk Exposure Analysis	38
6.	BEING INVOLVED IN THE AVIATION SAFETY COMMUNITY	38
7.	NOTES	43
7.1	Revision Indicator	43
APPENDIX A	SAFETY SIGNIFICANT EVENT REFERENCE LIST	44
APPENDIX B	QUALITATIVE RISK ASSESSMENT	68
APPENDIX C	QUANTITATIVE RISK ASSESSMENT	78
APPENDIX D	ROOT CAUSE (EVENT TREE) ANALYSIS	87
APPENDIX E	WEIBULL ANALYSIS	100
APPENDIX F	MONTE CARLO SIMULATION	118
APPENDIX G	RELIABILITY GROWTH MODELING	137
APPENDIX H	FLIGHT OPERATIONAL QUALITY ASSURANCE FOQA	145
APPENDIX I	MAINTENANCE ERROR DECISION AID (MEDA)	151
APPENDIX J	OPERATOR SERVICE BULLETIN PROCESS	188
APPENDIX K	MANUFACTURER SERVICE BULLETIN PROCESS FOR SAFETY RELATED SERVICE INFORMATION	193
APPENDIX L	AIRWORTHINESS DIRECTIVE DEVELOPMENT PROCESS	195
APPENDIX M	HAZARD TRACKING	199
APPENDIX N	LESSONS LEARNED	202
APPENDIX O	FAA AND EASA QUANTITATIVE RISK ANALYSIS METHODS AND GUIDELINES	209
Figure 1	Overview of the ongoing safety assessment process	11
Figure 2	Ongoing safety assessment process	12
Figure 3	Numerical risk assessment overview	19
Figure 4	Integrated ongoing safety assessment process	25
Table 1	Database access	31
Table 2	Safety related conferences	39
Table 3	Safety related websites	41

1. SCOPE

This document describes guidelines, methods, and tools used to perform the ongoing safety assessment process for transport airplanes in commercial service (hereafter, termed "airplane"). The process described herein is intended to support an overall safety management program. It is associated with showing compliance with the regulations, and also with assuring a company that it meets its own internal standards. The methods identify a systematic means, but not the only means, to assess ongoing safety.

While economic decision-making is an integral part of the safety management process, this document addresses only the ongoing safety assessment process. To put it succinctly, this document addresses the "Is it safe?" part of safety management; it does not address the "How much does it cost?" part of the safety management.

This document also does not address any specific organizational structures for accomplishing the safety assessment process. While the nature of the organizational structure is significant to the quality of a safety program, this document focuses on the functions to be accomplished and does not attempt to define what the structure should be. The intent is to leave the greatest amount of flexibility to the organizations that use this document.

1.1 Purpose

This document provides a systematic process to measure and monitor safety to help determine safety priorities and focus available resources in areas that offer the greatest potential to improve aviation safety. The current practice for ongoing safety assessment relies primarily on input from individual carriers or operators, with substantial involvement from the manufacturers, suppliers, airworthiness authorities, and other aviation service providers. There are variations in practices at all levels throughout the industry. Also, air transport carriers, air cargo carriers, and manufacturers each use their own methods for accomplishing safety assessment. It is felt that the creation of an industry practice will enhance consistency of approach in how airplane safety assessment is conducted and how airplanes are operated worldwide. This document is not a regulation. It is, rather, a compendium of best safety practices gathered together as a reference. It allows the users to compare their existing methods to those listed herein to seek improvements.

To improve safety during the complete airplane life cycle, it is not sufficient to assess the safety of the airplane only during its design phase. Ongoing airplane operations must be evaluated for safety (e.g., maintenance or operation procedures). The airplane is also evolving and changing during the "In-Service" phase (e.g., obsolescence, modifications). Differences exist or can develop between the assumptions made during the design phase and how the airplanes are actually operated and maintained. For these reasons, safety should be assessed also during the "In-Service" phase of the airplane life cycle. In order to do that, information must be collected, monitored and analyzed. A large portion of this needed information may already exist in an organization's maintenance or warranty information databases.

In addition to maintaining the safety of the airplane, there is also a need to enhance safety wherever possible. This means that the user must always be alert to the opportunity to advance safety where possible and feasible.

The transport airplane accident rate has improved since 1975; however, the number of airplanes has greatly increased and will continue to increase. The transport aviation industry provides the safest form of transportation in the world, but each accident generates tremendous negative effect. Thus, it is imperative to constantly improve. This can be accomplished by continuously improving what we do and what we accept as adequate.

This revision contains several new practices (e.g., the Transport Airplane Risk Analysis Method (TARAM), Safety Management System (SMS)) that did not exist at the time of the original publication.

1.2 How to Use This Document

The intent of this document is to identify typical activities, methods, and documentation that may be used to perform safety assessments for airplanes (including their associated systems and equipment) and user operations. The document describes a number of valid methods for resolution of safety issues, selection of actions, and their scheduling. The specific applicability and usefulness of the individual guidelines, methods, and tools will vary among organizations and from situation to situation. The user is not constrained to use all of the elements contained within this document. Each organization needs to establish which sections may prove helpful in improving or supplementing its existing safety-related practices. The guidelines, methods, and tools provided in this document are to be used in conjunction with other applicable guidance materials.

The appendices are not stand-alone documents, but rather are to be used in conjunction with the information contained in the basic document. The user is cautioned not to use the appendices independently of the basic document. Document users are also cautioned not to ascribe greater importance or validity to one method or tool presented in the appendices over another when addressing safety issues. No hierarchy is intended, either explicitly or implicitly, by the authors.

1.3 Intended Users

The intended users of this document include but are not limited to:

- a. Operators
- b. Manufacturers
- c. Equipment suppliers
- d. Modification or repair centers
- e. Airworthiness authorities

Anyone involved with the safety assessment and safety management of transport airplanes in commercial service may be a potential user.

2. REFERENCE DOCUMENTS, DEFINITIONS, AND ACRONYMS

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 Airworthiness Documents

AC 20-176A	Service Bulletins Related to Airworthiness Directives
AC 25.1309	System Design and Analysis, Advisory Circular
AC39-8	Continued Airworthiness Assessments of Powerplants
AC120-92B	Safety Management Systems for Aviation Service
AD FAA-IR-M-8040	Airworthiness Directives
AMC 25.1309	System Design and Analysis, Advisory Circular (was AMJ)
FAA Order 8110.107A	Monitor Safety/Analyze Data
ICAO Annex 8	Continuing Airworthiness of Aircraft
ICAO Annex 13	Accident Investigation
ICAO Annex 19	Safety Management
PS-ANM-25-05	Airworthiness Manual

2.1.2 Industry Documents

AIA Project Report High Bypass Ratio Turbine Engine Uncontained Rotor Events

ARP4754 Guidelines for Development of Civil Aircraft and Systems

ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

ATA Spec 100 Specification for Manufacturer's Technical Data

ATA Spec 111 Airworthiness Concern Coordination Process

CAAM 1 Technical Report on Propulsions System and Auxiliary Power Unit (APU) Related Safety Hazards

CAAM 2 2nd Technical Report on Propulsions System and Auxiliary Power Unit (APU) Related Safety Hazards

CAAM 3 3rd Technical report on Propulsions System and Auxiliary Power Unit (APU) Related Safety Hazards

MSG-3 Airline/Manufacturer Maintenance Program Development Document MSG-3

2.1.3 Military Publications

MIL-STD-882E Standard Practice for System Safety

2.2 Definitions

This section provides definitions for terms uniquely used in this document.

Note: Terms with an * are intentionally defined differently versus ARP4761 and ARP4754, as those documents apply to aircraft/system development.

ACCIDENT: An occurrence associated with the operation of an airplane, that takes place between the time any person boards the airplane with the intention of flight, until such time as those persons have disembarked, in which: Any person suffers death or serious injury as a result of being in or upon the airplane, or by direct contact with the airplane or anything attached thereto; the airplane received substantial damage; any damage is caused to the property of a third party. (NTSB)

ACCIDENT PREVENTION STRATEGIES: An ongoing process of developing lessons learned from past prevention events to identify strategies for preventing future accidents. Use of a prevention strategy approach has the potential of preventing accidents by identifying and removing one or more links in the accident chain.

AIRWORTHINESS: The condition of an item (airplane, airplane system, or part) in which that item operates in a safe manner to accomplish its intended function.

ANALYSIS: A detailed examination based on decomposition into simple elements.

APPROVED: Accepted by the certification authority as suitable for a particular purpose. (ICAO)

ASSESSMENT: An evaluation process which may include one or more types of analysis and experience.

AUTHORITY: The organization or person responsible within the State (Country) concerned with the certification of compliance with applicable requirements.

CANCELLATION: Elimination of a scheduled flight because of a known or suspected malfunction and/or defect. **Note:** Cancellation of any or all of the flight legs of a multi-leg flight constitutes only one cancellation (WATOG).

CERTIFICATION MAINTENANCE REQUIREMENT (CMR): A Certification Maintenance Requirement is a required periodic maintenance task established through formal numerical analysis to show compliance with certification requirements.

COMPLEXITY: An attribute of systems or items that makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.

COMPLIANCE: A timetable for performing specified corrective actions (e.g., schedule maintenance, inspections, part replacements, alterations, etc.) to alleviate an identified safety related problem.

COMPONENT: Any self-contained part, combination of parts, subassemblies, or units, which perform a distinct function necessary to the operation of the system.

CONFIGURATION DEVIATION LIST (CDL): An approved list of items, such as access panels, caps, fairings, etc., normally forming part of the airplane exterior profile, the absence of which do not prevent dispatch (WATOG).

CONFORMITY: Agreement of physical realization of the item with the defining document.

CONTROL PROGRAM: The combination of compliance schedule and corrective actions needed to alleviate an identified problem.

CREW: Crew includes but is not limited to, the following participants in the aviation system; flight crew, cabin crews, maintenance personnel, dispatchers and crew schedulers, and air traffic controllers.

CRITICALITY: Indication of the hazard level associated with a function, hardware, software, etc., considering abnormal behavior (of this function, hardware, software, etc.) alone, in combination, or in combination with external events.

DEFECT: State of an item consisting of the non-performance of specified requirements by a characteristic of the item. A defect may, but need not, lead to a failure.

DISPATCH RELIABILITY: The percentage of scheduled revenue flights that depart without incurring a technical delay or cancellation.

ERROR: An omitted or incorrect action by a manufacturer, crew member, or maintenance person, or a mistake in requirements, design, or implementation.

EVENT: An occurrence that is of interest for airplane safety.

EXTERNAL EVENT*: An occurrence that has its origin distinct from the airplane, such as atmospheric conditions (e.g., wind gusts, temperature variations, icing, lightning strikes), runway conditions, and cabin or baggage fires. The term is not intended to cover sabotage.

FAILURE: A specific way in which a system, equipment, item, or piece-part may fail.

FAILURE CONDITION: A condition with an effect on the airplane and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operation or environmental conditions. A Failure Condition is classified in accordance to the severity of its effects as defined in regulatory advisory circulars.

FAILURE EFFECT: A description of the operation of an aircraft, system, equipment, or an item as the result of a failure; i.e., the consequence(s) a failure mode has on the operation, function or status of an aircraft, system, equipment, or an item.

FAILURE MODE: The way in which the failure of an item occurs.

FAILURE RATE*: The gradient of the failure distribution function divided by the reliability distribution function at time t . Failure Rate = $F'(t)/(1-F(t))$. If the failure distribution function is exponential, the failure rate is constant and the failure rate can be approximately calculated by dividing the number of failures within a hardware item population, by the total unit operating hours. Note: Failure rate may also be expressed in terms of failures per flight hour or per cycle.

FLIGHT CYCLE: A completed take-off and landing sequence.

HAZARD: A condition resulting from failures, external events, errors, or a combination thereof where safety is potentially affected.

HUMAN FACTORS: The optimization of the relationship between people and their activities by the systematic applications of the human sciences integrated within the framework of systems engineering.

INCIDENT: An occurrence other than an accident, associated with the operation of an airplane, which affects or could affect the safety of operation. (NTSB)

INFLIGHT SHUTDOWN: An engine shutdown which occurs at any time an airplane is airborne or has been committed to becoming airborne.

ITEM*: One or more hardware and/or software elements treated as a unit.

MALFUNCTION*: The occurrence of a condition whereby the operation is outside specified limits.

MASTER MINIMUM EQUIPMENT LIST (MMEL): A list of equipment and functions that need not be operative for safe flight and landing based on stated compensating precautions created during airplane type certification.

MEAN TIME BETWEEN FAILURES (MTBF)*: A performance figure calculated by dividing the total unit flying hours (airborne) accrued in a period by the number of unit failures that occurred during the same period.

MINIMUM EQUIPMENT LIST (MEL): An approved list of items that may be inoperative for flight under specified conditions cooperatively created by operators and regulatory authorities.

PARAMETER: A measurable or calculated quantity that varies over a set of values.

PILOT REPORT: Suspected or known malfunction or unsatisfactory condition entered by the flight crew into the airplane logbook and which requires maintenance action.

PROBABILITY: A measure of the likelihood of occurrence. When expressed qualitatively, words such as low, medium, high are frequently used. When expressed quantitatively, probability is the limiting value of the relative frequency of occurrence of events of interest, when the limit exists. Its value lies between 0 and 1.

QUALITATIVE: Those analytical processes that assess airplane safety in a subjective and non-numerical manner.

QUANTITATIVE: Those analytical processes that apply statistical and data based methods to assess airplane safety.

REDUNDANCY: Multiple independent means incorporated to accomplish a given function.

RELIABILITY: The probability that a system, equipment, or hardware item will perform a required function under specified conditions, without failure, for a specified period of time.

REVENUE FLIGHT: A flight intended to generate either passenger or freight revenue (or both).

RISK:* The frequency (probability) of occurrence and the associated level of hazard. Perceived risk is risk as seen intuitively by individuals. Predicted risk is predicted analytically from models structured from historical studies.

ROOT CAUSE: The initiator of a sequence.

SAFETY ASSESSMENT*: Safety Assessment is the monitoring, identification, assessment, and prioritization according to hazard/severity level and probability of occurrence of risks associated with operations in a company. A process dedicated to assuring that risk is identified and managed properly within established limits; a process of identifying, estimating, and prioritizing each risk; assessment of accident and injury, and determining if action should be considered.

SAFETY MANAGEMENT: Safety Management is the decision-making process involved with determining and implementing what level of risk and cost is acceptable in a company and controlling the risk to that level.

SERIOUS INCIDENT: Any event involving the operation of an airplane other than an accident where the event, or the event coupled with any other reasonably probable second event, has the direct potential to result in an accident. (ICAO)

SUBSTANTIAL DAMAGE: Damage or damage failure which adversely affects the structural strength performance, or flight characteristics of the airplane, and which would normally require major repair or replacement of the affected component.

(Not considered substantial damage are engine failure or damage limited to an engine if only one engine fails or is damaged, bent fairings or cowling, dented skin, small punctured holes in the skin or fabric, ground damage to rotor or propeller blade, and damage to landing gear, wheels, tires, flaps, engine accessories, brakes, or wing tips.) (NTSB)

SYSTEM: A defined combination of subsystems, equipment, or items that perform one or more specific functions.

VALIDATION: The determination that the requirements for a product are sufficiently correct and complete. For example; "Did I build the right house?" (with respect to my original expectations).

VERIFICATION*: The evaluation of an implementation to determine that applicable requirements are met. For example; "Did I build the house right?" (in accordance with the drawings).

2.3 Acronyms

A4A	Airlines for America
AC	Advisory Circular
AD	Airworthiness Directive
AIA	Aerospace Industry Association
AMOC	Alternative Means (Methods) of Compliance
AMSAA	Army Material Systems Analysis Agency
ARP	Aerospace Recommended Practice (SAE)
ASIAS	Aviation Safety Information Analysis and Sharing
ASRS	Aviation Safety Reporting System
ATSB	Australian Transport Safety Board
BASIS	British Airways Safety Information System
CAAC	Civil Aviation Administration of China
CAAM	Continued Airworthiness Assessment Methodologies
CDF	Cumulative Distribution (Density) Function
CDL	Configuration Deviation List
CFR	Code of Federal Regulations
CMR	Certification Maintenance Requirement
COS	Continued Operational Safety
DOE	Department of Energy
EAD	Emergency Airworthiness Directive
ECS	Electronic Control System
ETOPS	Extended Twin-Engine Operations
FAA	Federal Aviation Administration

FMEA	Failure Mode and Effect Analysis
FOQA	Flight Operational Quality Assurance
GAIN	Global Aviation Information Network
HCF	High-Cycle Fatigue
HF	High Frequency (VHF - Very HF)
IAR	Immediately Adopted Rule
ICAO	International Civil Aviation Organization
LCF	Low-Cycle Fatigue
LL	Lessons Learned
LRU	Line Replaceable Unit
MCAI	Mandatory Continuing Airworthiness Information
MEDA	Maintenance Error Decision Aid
MEL	Minimum Equipment List
MMEL	Master Minimum Equipment List
MRB	Maintenance Review Board
MSG-3	Maintenance Steering Group 3
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
NPRM	Notice of Proposed Rulemaking
NTSB	National Transportation Safety Board
OEM	Original Equipment Manufacturer
OHL	Operator Hazard Level
SB	Service Bulletin
SDR	Service Difficulty Report
SMS	Safety Management System
SRA	Safety Risk Analysis/Assessment
TARAM	Transport Airplane Risk Assessment Method
WATOG	World Airlines Technical Operations Glossary

3. SAFETY PROCESSES IN THE OPERATING FLEET

Ongoing safety management is an activity dedicated to assuring that risks are identified and unacceptable risks are eliminated or controlled. As such, the ongoing safety management process is a systematic and logical approach.

A robust Safety Management System (SMS) will help ensure that risks are identified and properly eliminated or controlled. There are many sections within ARP5150A that can help satisfy the requirements of SMS, including its Safety Risk Management (SRM) and Safety Assurance (SA) elements.

Removing the decision-making step from the safety management process leaves the safety assessment process, which this document describes. This process is accomplished by professionals whose job it is to handle the technical details of safety assessment. Results from the ongoing safety assessment process are provided for decision-making in safety management. This management decision-making is accomplished by those individuals responsible for choosing which projects are appropriate for the expenditure of company assets.

Safety is not self-sustaining. When an airplane is delivered and is in its pristine condition, it has an initial level of safety. As airplanes are operated, the level of safety is maintained through a continuing process of monitoring service experience, identifying safety-related issues and opportunities, and addressing these issues or opportunities through appropriate product or procedural changes.

3.1 Overview of the Ongoing Safety Assessment Process

The Ongoing Safety Assessment Process continues the effort started during the airplane design phase. It begins with the introduction of the new airplane and continues until the airplane is retired from service.

The Ongoing Safety Assessment Process includes three objectives:

1. Maintain the airworthiness (certification) of the airplane:

In-service events are assessed based on effects on the level of safety intended in the certification process.

2. Maintain the safety of the airplane:

In-service events are assessed against the internal safety objectives of the organization.

3. Improve the safety of the airplane:

In-service events are assessed to identify opportunities to decrease their number or to surpass the safety objectives of the organization.

The safety assessment process is expected to be continuous, iterative, and closed-loop. When an event is identified, assessed and action implemented, the monitoring continues, to validate the effectiveness of the action.

The safety of the airplane depends on numerous factors, including the original design, manufacturing, flight crew and maintenance actions, operation effects, quality of parts, modifications, environment, and airplane aging.

Each user of this document is encouraged to develop their own Ongoing Safety Assessment process and continuously adapt it to their specific operating needs and criteria. Communication with other operators, suppliers, and manufacturers is advantageous throughout the process.

Figure 1 identifies a recommended high-level process for ongoing safety assessment. This generic process consists of five high level steps:

1. Establish Monitor Parameters
2. Monitor for Events
3. Assess Event and Risk
4. Develop Action Plan
5. Disposition Action Plan

“ESTABLISH MONITOR PARAMETERS” starts with determining the company specific safety structure, objectives, and goals. This process also establishes the monitoring parameters and their values.

“MONITOR FOR EVENTS” is the continuous process of looking for events of concern. This monitoring is based on the parameters established in the previous step.

“ASSESS EVENT & RISK” is the process initiated when an event is detected. This includes assessment of the event sufficient to determine if the event is really of concern. It also includes a preliminary determination of risk for use in prioritizing initial expanded evaluation and action plan development. Based on the seriousness of the event and the initial risk evaluation, a more detailed and complete risk assessment may be performed.

“DEVELOP ACTION PLAN” is the process that establishes the correction or improvement, such as a design change, or a change to operations, maintenance, or training procedures for the event identified. The action plan may not be needed if the event is determined to be sufficiently benign.

“DISPOSITION ACTION PLAN” is the evaluation and/or implementation of the action plan. This may include determination of whether or not the action will be implemented and the prioritization, scheduling, and implementation of that action. Once the action is completed, or when the determination is made not to implement the action, the process returns to the normal state of monitoring for events. In some cases, revision or update of the parameters monitored may occur as a result of the event or the action implemented.

3.2 The Ongoing Safety Assessment Process

A further decomposition of the high-level process (Figure 1) is shown in Figure 2. The process shown in Figure 2 represents a recommended iterative process within each organization. Each user of this document is encouraged to tailor this process to meet their specific operations. The following sections describe each ongoing iterative safety assessment process steps shown in Figure 2.



Figure 1 - Overview of the ongoing safety assessment process

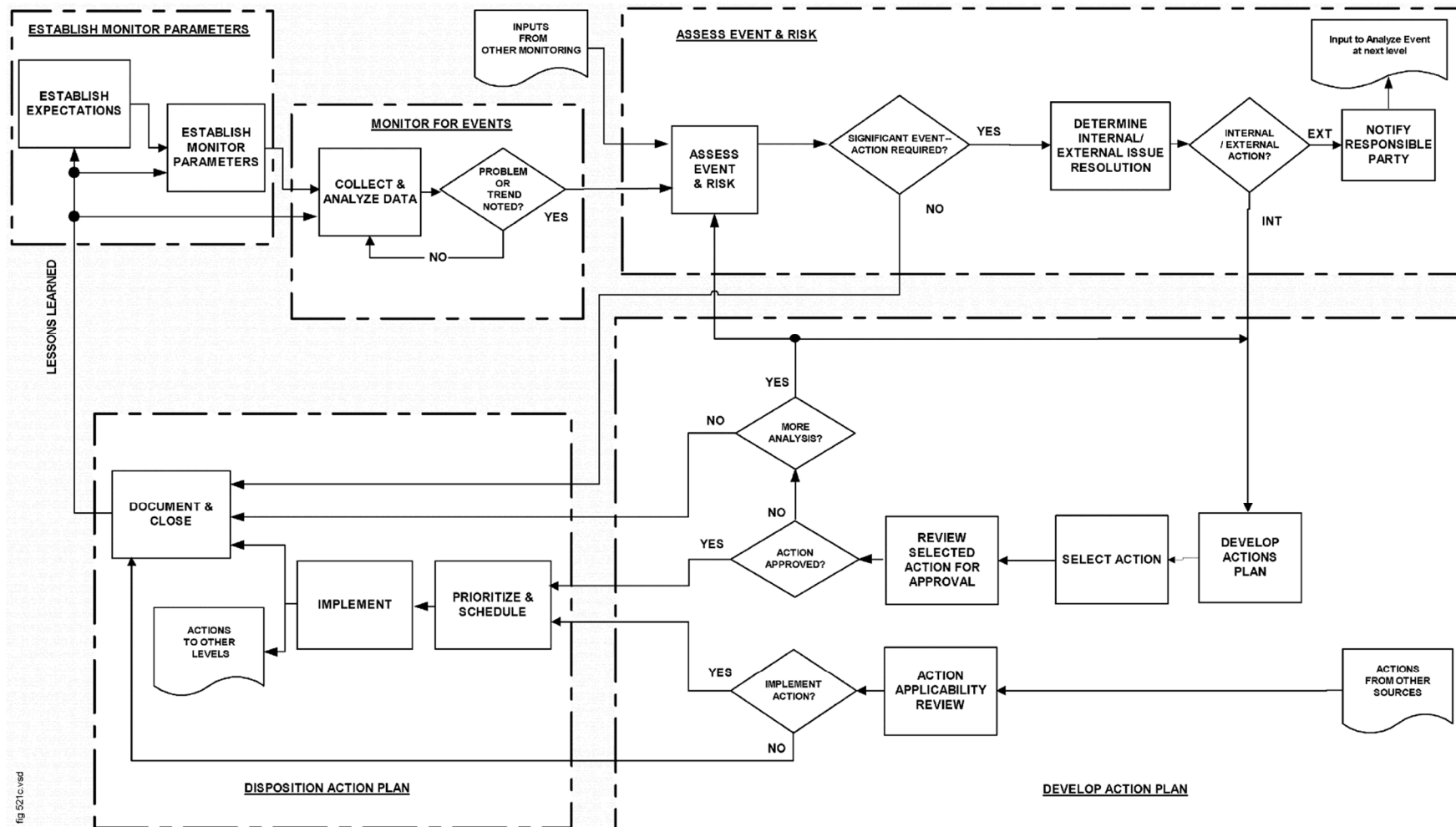


Figure 2 - Ongoing safety assessment process

3.2.1 Establish Monitor Parameters

The “ESTABLISH MONITOR PARAMETERS” phase shown in Figure 1 is expanded to “Establish Expectations” and “Establish Monitor Parameters” activities.

3.2.1.1 Establish Expectations

There are two basic aspects of the “Establish Expectations” step. The first of these is developing organizational structures and philosophies when initiating this process. This should include establishing the safety objectives and guidelines for the organization. The second is developing operational expectations for each specific fleet. This activity consists of determining what the day-to-day expectations of operation are, and what types of operations and performance will or will not be accepted within the fleet.

“Establish Expectations” encompasses the establishment of the company safety philosophy, assessment of the role of safety within the company structure, and the company’s definition of acceptable risk and performance levels. This company structure may vary from a structured formal safety organization to an informal structure. The safety organization should be sufficiently autonomous to ensure that it can influence the established safety philosophy.

There are at least two levels of expectations. The first are requirements imposed by the regulatory agency, which establish a minimum level of safety for operation. The second is the user’s own expectations, which may go beyond the requirements of the regulatory agencies. These internally imposed expectations may include parameters or criteria not covered by regulations, or levels of risk lower than required by regulations. The requirements and expectations may be based on a number of factors, including the following:

- a. Basic airplane requirements
- b. Safety analyses
- c. Regulatory reporting requirements
- d. Operational characteristics (e.g., cargo carriers versus passenger carriers or Cat I versus Cat IIIb)
- e. Airplane maintenance programs
- f. Environmental conditions of operation (e.g., tropical versus arctic operations)
- g. Experiences identified through previous use of the process (i.e., continuous improvement)
- h. Related industry accidents and incidents (where data is available)
- i. Lessons learned

The fleet specific expectations are passed on to the “Establish Monitor Parameters” phase of the process.

Once established, these expectations should be reviewed and adjusted whenever the user’s operation changes significantly or when external circumstances indicate the need for revision. Lessons learned from service experience, relevant certification assessments, post certification testing, product evaluations, and new technologies may also lead to the need for revisions of these expectations.

3.2.1.2 Establish Monitor Parameter Activities

The “Establish Monitor Parameters” step builds upon the expectations previously established. This step develops the information or data that should be collected, how it will be collected, and how it will be compared to expectations. This may vary from a minimum of existing regulatory-reportable issues to extensive data gathering and analysis programs. The exact parameters to be selected should be based on the level of the ongoing safety assessment process desired by management. The selection of specific parameters will be influenced by (among other things) the availability of data. Communication among the various organizations is beneficial in establishing appropriate parameters.

Appendix A provides an example list of airplane safety-related parameters and events that may be used as a starting point in the establishment of these parameters. In order to perform an effective ongoing safety assessment, many different types of data will have to be collected and analyzed. Section 4 provides more information on the types of data available to an organization and the sources from which the data may be obtained.

There are typically two types of parameters that are monitored. One type is the monitoring requirements generated as part of certification and identified in the Maintenance Review Board (MRB) document and subsequent Airworthiness Directives (AD). A second type is results from the user's own assessments (for example, an airline maintenance program may include a component functional check or removal at a specific interval).

Certain regulatory reporting requirements are called out in 14 CFR, 14 CFR Parts 121.703, 121.705, and 121.704. Parameters that may be required to be monitored include: engine overtemps, overweight landings, Service Difficulty Reports (SDRs), etc.

Based on the review of required reporting events described above, conditions may warrant the need for additional monitoring to help determine the event occurrence rate and the extent of the population at risk of the event.

The operator may also choose to monitor performance to assist in detecting problems before a serious event occurs. Monitoring the operation of specific systems can validate that their failure and availability rates are consistent with the supplier's or operator's expectations. While the occurrences of less-significant failures may be obvious to an operator because of their impact on reliability and the cost of operation, the operator may not be aware of more-significant failure conditions to which these failures contribute. Although it may be difficult for an original equipment manufacturer (OEM) or supplier to gather the data required to monitor the rate of occurrence of less-significant failures, this task should be accomplished whenever possible. Proactive monitoring of these lower events may identify potential problems early and allow for action to be taken to prevent more-serious events. This activity would be particularly effective at the OEM and supplier levels, as the action can be taken across on the affected worldwide fleet and not just within one operator's organization. It is therefore important that, where applicable, monitoring parameters for these lower-severity events be established at this stage.

As the Ongoing Safety Assessment process matures within an organization, the data being monitored, collection methods, and comparison processes should be continuously reviewed for the opportunity to make safety improvements. Continued service experience, new assessments, or post design evaluations are sources for lessons learned material. Lessons learned effects on the monitoring process are contained in 3.2.6 and Appendix N.

3.2.1.3 Monitoring Effectiveness of Previous Actions

After establishing the initial maintenance program for a given airplane, the operator, through its reliability program, continues to monitor the effectiveness of the program for the desired purpose of maintaining the airplane in a safe condition. The following are several means by which this is achieved.

Once actions are initiated to correct a problem, a follow-up validation process should be set up to monitor the implementation and determine effectiveness of the actions. This follow-up process may be accomplished by comparing pre- and post-action conditions of the systems affected by the correction. The frequency of comparison should be based upon probability and severity. During this post implementation review, a re-examination of the preliminary findings (e.g., teardown reports) may be accomplished. This verifies the implemented action eliminates the problem and that the assumptions used during the analysis are valid.

Adverse experience that deviates significantly from expectations or assumptions is grounds to revisit the safety assessment to determine which of the underlying assumptions are faulty, and whether additional actions are necessary. Since the immediate, short-term action is rarely expected to be the complete reaction to the problem, a complete validation of the effectiveness of any immediate action is likely not feasible prior to additional action being taken. Field experience and inspection results should continue to be monitored so that the new data acquired by interim action can be used to verify the effectiveness of the corrective action program. Final action carries with it an assumption that the failure mode has been effectively eliminated or mitigated; field experience should be tracked to validate this assumption. Care must also be taken to ensure that any unforeseen adverse impacts of actions are identified and evaluated.

Review of inspection findings allows for monitoring the effectiveness of the maintenance program. By reviewing the discrepancies generated by the performance of a regular task, the operator is able to get a good idea if the task itself and the interval at which it is performed are appropriate. For example, if too many discrepancies are reported against a specific task, the interval may need adjusting to a lower level check or the scope of the task may need to be broadened, so that any deterioration may be identified prior to a component or structural member needing replacement.

The reliability function also looks at the discrepancies discovered through unscheduled maintenance. By analyzing these discrepancies, recommended additions or changes to the existing maintenance program may be identified. Unexpected component removals for cause are indications that an adjustment to the maintenance task or interval is likely required.

The various engineering groups within an operator's organization may also play an important role in how effective a maintenance program is by continuously reviewing the various Service Bulletins (SBs) and Service Information Letters (SILs) issued by the manufacturer and the component vendors. These reviews establish the benefit of the SB recommendations to the operator's operational and maintenance procedures.

Once the expectations and monitoring parameters have been established, they are then used during the succeeding "MONITOR FOR EVENTS" step.

3.2.2 Monitor for Events

The "MONITOR FOR EVENTS" step consists primarily of the "Collect & Analyze Data" process.

An event is an occurrence. An event may be of interest by itself; e.g., an engine shut-down, or it may be of interest only in combination with other events that may or may not have happened at the same time; e.g., failure of one navigation receiver. An event may also be an operations or maintenance error. An event may or may not be significant for airplane safety. An event may be a single occurrence or a set or collection of separately identifiable occurrences that, for convenience of discussion and analysis, are thought of as a single event.

Monitoring for events encompasses two related, but distinct, elements: collecting and analyzing data, which monitors for previously unidentified or analyzed events of concern, and monitoring the effectiveness of previous actions, which monitors for events that have been already been evaluated through the process.

3.2.2.1 Collect & Analyze Data

The intent of the "Collect & Analyze Data" element of Figure 2 provides continuous monitoring of the actual operations to assess compliance with expectations. In this step, the data available to monitor any parameters defined in the "Establish Monitor Parameters" step should be obtained and analyzed. It is during the collection and analysis of this data that potential problems and trends will be identified. The cost of data collection and analysis is relatively low when compared to the potential cost of lost assets and equipment.

The following bullets highlight some example conditions that may be observed:

- Analysis of expected events occurring more frequently than anticipated provides for a comparison of performance data versus expected or acceptable frequency of occurrence for each event defined in the "ESTABLISH MONITOR PARAMETERS" phase. Any levels of occurrence closely approaching or exceeding the expected event's level of frequency indicate increasing potential for problems. These types of events may be monitored by reviewing the data results from scheduled airplane checks (sometimes called check reviews), and data from unscheduled maintenance (called reliability reports).

- If an unexpected or previously unknown event is detected, new parameters for this event should be established and added to the monitoring list. This event is then carried forward to “Assess Event & Risk.”
- The occurrence of minor events that could lead to increased risk should also be tracked to note any adverse trends. Minor events are not by themselves of concern, but may have more serious effects when combined with other events. When an adverse trend is detected, it should be investigated to determine if the trend indicates a safety concern. These types of events may be monitored using airplane reliability reports, employee suggestions, customer issues or Flight Operational Quality Assurance (FOQA) reports (see Appendix H).

It is recommended that each organization establish a formal means of collecting, summarizing and distributing the results of the “Collect & Analyze Data” element. The importance of accurate data should be emphasized. (Existing reliability programs may be extendible to encompass data collection for safety monitoring.)

Where no problem or trend is identified, the process continues in the “Collect & Analyze Data” element. When the analysis identifies a potential problem or trend, the data is summarized for use of the “ASSESS EVENT & RISK” phase of the process.

3.2.3 Assess Event & Risk

Once a potential problem or trend has been identified, either as a result of internal data collection and analysis or from an analysis performed by an external source, the “ASSESS EVENT & RISK” is initiated. This process develops a sufficient level of understanding of the event and its cause(s) to determine the possible consequences and assess the associated risk. Once these are known, a decision can be made as to whether or not the event warrants further action. If it is decided that the event does not warrant further action, the process should be recorded in the “Document & Close” step. If an event warrants further action, the appropriate organization(s) required to develop the action should be determined. If it is discovered that the problem requires external action, the responsible party should be notified of such action in a timely manner. If internal action is determined, then proceed to “DEVELOP ACTION PLAN.”

The “ASSESS EVENT & RISK” phase shown in Figure 2 is expanded to “Assess Event & Risk,” “Determine Internal or External Issue Resolution,” and “Notify Responsible Party.”

3.2.3.1 Assess Event & Risk

The assessment of the event and subsequent risk provides information that defines the magnitude of a specific safety issue. It also provides risk mitigation and optimization of inspection and modification programs designed to control in-service safety related problems. This assessment is performed to decide if an issue is a safety problem or to provide visibility of major risk issues. Risk assessments may be qualitative or quantitative and should always include a determination of severity and the probability of occurrence.

As a general principle, there should be an inverse relationship between severity and probability. Thus, safety issues of higher severity should be lower in probability.

In order for an organization's ongoing safety assessment process to be successful, it is essential that the “Assess Event & Risk” step effectively prioritizes the problems that occur so that the more critical problems are dealt with first. Although there are many prioritization schemes in use throughout the aviation industry, these schemes generally fall into three broad groups. These three groups differ based on what information is used as prioritization criteria.

Level 1 (Hazard Level): Severity (how bad is it?)

Level 2 (Risk): Severity + Probability (how bad is it, and how likely is it to happen?)

Level 3 (Fleet Risk): Severity + Probability + Exposure (how bad is it, how likely is it to happen, and what is the size and utilization of the affected fleet?)

An effective prioritization scheme evolves as the risk assessment task progresses. At each step in the review of a problem, it is important that priorities be established based on all relevant information available at the time. This evolution can be accomplished by moving from a Level 1 prioritization scheme to a Level 2 prioritization scheme, and then to a Level 3 prioritization scheme as probability and exposure information is collected.

3.2.3.1.1 Assess Event

The first step is to assess the observed event. Understanding the event obviously includes a review of the data obtained from the observed event, but also may entail searching accident and incident databases for similar occurrences of the event and potential problems resulting from it. These databases may be the user's own data sources, data shared with other operators on a limited basis, or industry, regulatory authority, government, or insurance company data. The search should be broad enough to detect similar problems in similar products or functions and should cover other airplane types to determine if the concern is an airplane or fleet specific issue, or a more general issue. Communication with other users of the equipment, the equipment manufacturer or airplane manufacturer may assist in this analysis.

In judging the severity of the event, it is important to understand the actual consequences that the observed event had on airplane operation. It is even more important, however, to understand potential airplane consequences if the event had occurred during more vulnerable circumstances. The event may be considered more severe if the consequences would be worse under different operating conditions (e.g., flight phase, environment).

A Level 1 problem prioritization scheme is most useful during the early stages of the safety assessment process, when little is known other than the observed or potential consequences to the airplane and passengers. The problem is assigned a severity category based solely on the seriousness of those consequences. Many different schemes for classification of safety events are used successfully within the aviation industry. The success of a particular classification method depends not so much on its specific details as on it being a formal and consistent part of an organization's safety process. Appendix B provides more details on the various event severity categorization schemes in use within the aviation industry.

It is also important at this stage to identify if the event would have been more severe had it occurred in combination with other failures. Time should be taken to identify all more severe failure conditions to which the observed event contributes. During the risk assessment phase, it is important to consider how the probability of the observed event influences the probability of these more severe failure conditions.

Research of the root cause should consider all known occurrences and initiators of the potential problem. Analysis of the causes of an event should consider:

- a. Aspects of the original design and design intent
- b. How the product or function's usage may have changed beyond initial design objectives
- c. Manufacturing aspects
- d. Specific utilization of the product or function relative to its intended usage instructions
- e. Maintenance of the product or function
- f. Complexity of the system
- g. Associated procedures and training
- h. Clarity/accuracy of the manuals and procedures
- i. Other applicable considerations

During the analysis of root causes, it may be necessary to define and gather additional data regarding sub-level events or failures leading to the condition. These issues could be failures or failure rates of other equipment or functions contributing to the event of concern. Where product manufacturer's installation, usage guidance instructions, and/or operational and operating environment assumptions are available, analysis of the actual installation and usage against those assumptions may aid in detecting and identifying characteristics leading to the unexpected operation or function. This review may identify discrepancies in modification or expected functionality.

A variety of tools may be used in determining the event extent, event causes, consequences of events, and event severity category. Section 5 presents a detailed description of some selected tools and their usage.

The assessment of the root cause should not be limited to the use of the analytical tools referenced above. Where possible, information should be obtained from computer fault logs, lab testing of suspected components, etc. A Line-Replaceable Unit (LRU) with a hard failure or a failure that can be duplicated either on the airplane or on the bench can provide a wealth of information to OEM or airplane manufacturer during the investigation. The ideal investigation may have these activities occurring in conjunction with the analytical process.

Again, the objective of this step is to gather information on the scope, causes, and severity of the event, not to produce an action for the event. The output of this phase is an overall understanding of the event suitable to form the basis of the Risk Assessment.

3.2.3.1.2 Assess Risk

The Risk Assessment begins once a potential problem has been identified from the event and should be refined as its scope, causes and severity are known. As the investigation progresses, the next step is usually to assess the probability of the problem. This assessment typically describes the probability of occurrence of the problem on per flight hour, although it can also be expressed on per flight cycle or other relevant time interval. The assessment can be either qualitative or quantitative. A Level 2 prioritization assigns a risk category based on both the severity category and this probability. One usage of this level is evidenced when two problems may have consequences of equal seriousness; using a Level 2 categorization, the problem with higher probability can appropriately be given higher priority.

Risk assessment factors may include failure modes, failure classifications, failure probability distributions, conditional probabilities, probability of detection at inspection, size of the "at risk" population, operational/maintenance constraints, and candidate actions.

The risk assessment should be verified by comparison with experience to date wherever possible. A team of experts from appropriate disciplines should review critical elements of the risk assessment.

Operators tend to use qualitative estimates of the probability of occurrence of a problem. Information provided by operators can be critical to the manufacturer's analysis of an event. The OEMs generally perform quantitative analyses since they have detailed knowledge of the equipment design. The OEMs may also have access to data on their worldwide fleet, which allows for a more accurate calculation of the event probability. Appendix B describes qualitative risk assessment methods, while Appendix C describes quantitative risk assessment methods, and 3.2.3.1.2.1 provides general guidance on possible processes in creating a quantitative risk assessment.

3.2.3.1.2.1 Developing a Risk Model

One of the first steps in creating a risk model is to determine what analytic method you should use, based on available data. Figure 3 (below) provides a sample procedure.

Step 1: Define the Failure. The failure criteria must be clearly and unambiguously defined. This definition must determine a clearly identifiable point in the propagation of the failure sequence; e.g., the first detectable crack, or cracking sufficient to cause detachment of blade airfoil. A clear engineering understanding of the problem to be modelled is required, and whether the failure is dependent on operating time or cycles.

Step 2: Determine the conditional probabilities and severity factors to relate the event to the possible consequences. This can be done various methods, such as a Markov Chain, historical rates, CAAM data, Event Tree, Engineering judgement, etc.

Step 3: Determine how many failures there have been to date.

Step 4: Determine if failure time (hours/cycles, etc.) for the individual components is available.

Step 5: Determine if failure calendar time is available. This will determine whether there is sufficient information to create a Weibull with estimated failure/suspension times/cycles, or if a Crow-AMSAA would be preferred.

Step 6: Determine if suspension time/cycles for the individual components is available or can be estimated. This will determine the recommended method.

Step 7: Once the current failure rate is modeled, determine if the failure rate is mitigated via some type of inspection/replacement process. A Monte Carlo simulation may be used to model the replacement/inspection risk.

Step 8: Evaluate the current risk versus the appropriate risk criteria to determine whether or not it is acceptable.

Step 9: If the current risk is not within limits, calculate the Risk Reaction Time and determine what method will be used to mitigate risk to acceptable levels (for example part replacement, inspection, redesign, etc.).

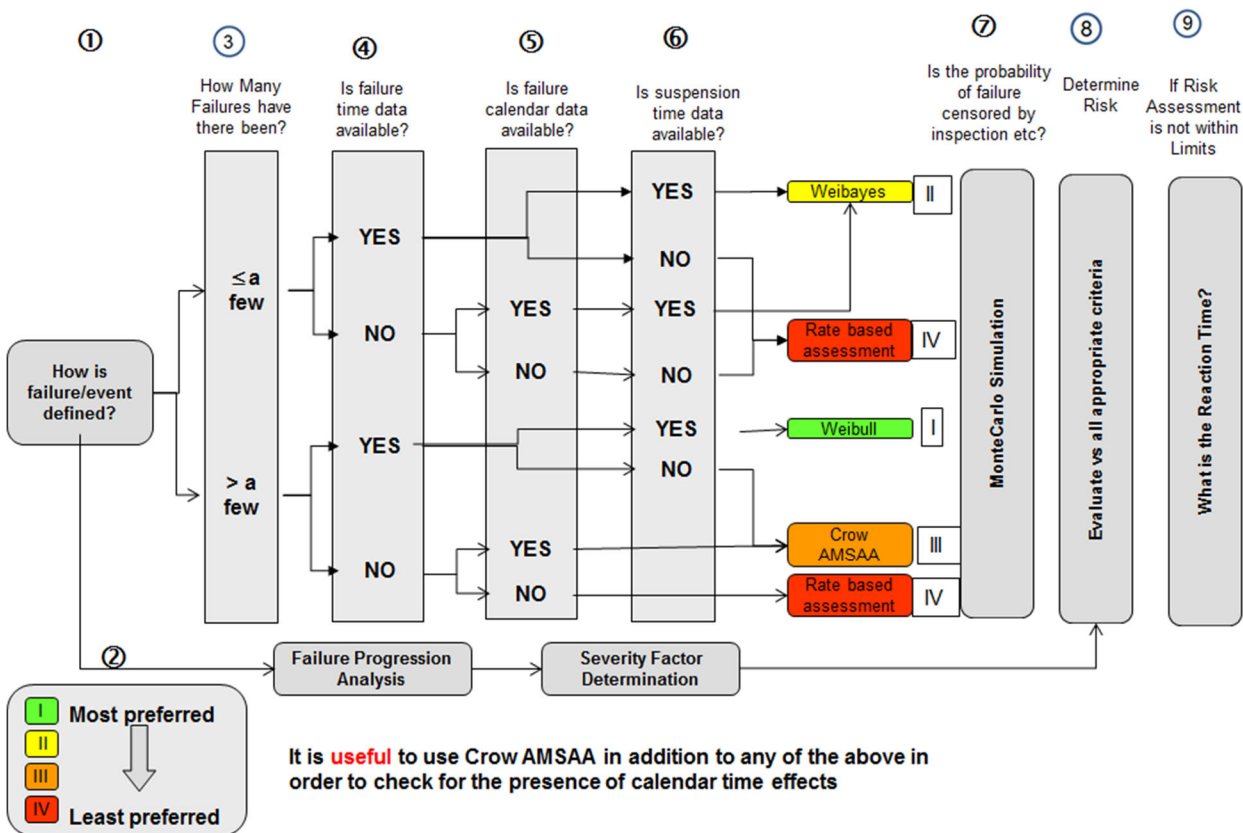


Figure 3 - Numerical risk assessment overview

With the initial risk assessment completed, the problem may be evaluated to determine if action is required, and, if so, to assign a priority to the resolution. Paragraph 5.4 describes two processes that may be used in scheduling implementation of corrective actions. It may be beneficial to establish a means of tracking the investigation or issue in order to ensure that the problem is resolved in a timely manner. One method of accomplishing this is to generate Hazard Summary and Hazard Tracking sheets. The Hazard Tracking Sheet and the Hazard Summary List are further discussed in Appendix M. A variety of tools may be used in assessing the risk of potential problems. Some of these tools and locations of information on these tools is provided in Section 5. As the study progresses further, information on the size of the affected fleet typically becomes available. Based on the fleet size and utilization, the future exposure can be determined. A Level 3 problem categorization can then be done, which assigns a fleet risk category based on severity, the per flight hour probability, and the future exposure. In effect, the Level 2 evaluation done earlier is extended to provide a "per fleet" probability. One usage of this level is evidenced when two problems may have equal severity and equal probability per flight hour; using a Level 3 categorization, the problem with the largest affected fleet (i.e., exposure) can appropriately be given higher priority.

The problem may apply to other airplane types/models as well. An assessment should be made to determine if other types may have the same problem. If so, the other types should be included in the "fleet" being considered.

The initial use of a risk assessment is to help provide an understanding of the magnitude of a specific problem. However, it will be necessary to revisit the risk assessment later to help judge the adequacy of proposed action plans. A specific proposed action plan will reduce the risk by reducing the probability or, alternatively, by lessening the severity (or possibly both). When there are alternative action plans proposed, risk assessment can be used to rank the plans, based on how much each plan reduces the probability or severity of failure.

An action plan, which provides adequate risk reduction for an individual “corrected” airplane, may still be inadequate if the action is implemented into the fleet too slowly. This can be judged via a “fleet risk” assessment, which expands the probability assessment to consider fleet size and the implementation schedule. When alternative implementation schedules are proposed, risk assessment can be used to rank the proposed schedules, based on how much and how quickly each proposed schedule reduces future exposure and risk.

Once the initial assessment of the event and risk has been completed, a determination of whether to accept the risk or initiate an action must be made. This determination should be accomplished by presenting the results of the event and risk assessment to the organization’s management and technical experts. As a practical matter in making decisions, economic impacts should also be considered by the organization’s management. These impacts are outside the scope of this document. The determination may include identification of additional monitor parameters as input to the “Establish Monitor Parameters” step.

If it is determined not to produce a corrective action for the event, the process proceeds to “Document & Close.” If the decision made is that the situation does warrant continued investigation, a determination must be made whether the responsibility to provide the action is internal to the organization or external.

3.2.3.2 Determine Internal/External Issue Resolution

If the organization identifying the event has the capability and responsibility to pursue the action, it does so, continuing through the process to the “DEVELOP ACTION PLAN” phase. If not, the responsible, external organization is determined.

3.2.3.3 Notify Responsible Party

Once the responsible organization has been identified, they are contacted and they begin evaluation with the “ASSESS EVENT & RISK” step within their process. Quite often the investigation continues with participation by more than one organization. For example, consider that an incident occurs in the field. The operator will assess the event and risk and may contact the OEM. It is important to understand that the processes between originator and actioned organizations are now interlinked. The originator may wish to coordinate and track the actioned organization's progress toward a timely action resolution. Good communication between all involved organizations is essential. Actions formulated by the external organization will reenter the originators safety assessment process at the “Action Applicability Review” step.

3.2.4 Develop Action Plan

The process continues with the responsible organization addressing the event in their respective “Develop Actions Plan,” “Select Action,” and “Review Selected Action for Approval” processes.

3.2.4.1 Develop Actions Plan

The “Develop Actions Plan” step encompasses any further research into event causes and the development of one or more potential actions. This should include risk assessment of the potential actions.

It may not be practical to develop actions for all problems simultaneously due to limited resources. Therefore, the organization must assign priorities based on their internal problem tolerance and possible regulatory oversight. These priorities allow an allocation of resources that focuses on safety-critical items first and the acknowledgment and tracking of operator-sensitive issues for review at a later time.

When developing an action, it is important to understand the root cause of the problem. This root cause may identify multiple failures that occurred over time or simultaneously and the sequence of these failures that led to the ultimate problem. By understanding these issues the responsible department can take each one of the failures and break it into two basic groups: hardware/software and human factors. Using these basic groups the action can be identified that best fits the needs of the user. Generic resolutions for these groups can be: replacement or redesign of an item, increase inspection frequency, retraining the operators, changing of a maintenance practice or addition of a system. It is desirable to focus on resolutions that reduce the probability of human error.

These resolutions should take into account the risk severity, the acceptable level of process or design change and the speed of risk reduction. In each case, the incremental risk associated with the interim solution should be reviewed, such as those associated with higher flight crew workload.

When the resolution is identified, it should be developed in detail, tested to verify the action and validate its effectiveness. The documentation should include the rationale and benefits of the proposed recommended actions (e.g., power the airplane down every “n” hours to force a power-up test to activate and verify absence of latent faults, thus maintaining the validity of the safety analysis).

3.2.4.2 Select Action

“Select Action” consists of evaluating the action options and identifying those with acceptable levels of safety. This step will usually involve presenting the action(s) for organizational approval. Typically, presentations are made by technical expert(s) to a review board or management position and should include a statement of the issue or concern, historical background, risk analysis results and assumptions, actions already taken and recommended future actions.

3.2.4.3 Review Selected Action for Approval

Based on the presentations made by the technical experts, the organization’s management or review board approves or rejects the proposed action. As a practical matter in making decisions, economic impacts would also be considered by the organization’s management. These impacts are outside the scope of this document.

For those actions approved by the organization’s review board or management, the implementation method depends upon the type of organization (e.g., Engineering Order (EO) for operators, Service Bulletin (SB) for manufacturers, Airworthiness Directive (AD) for regulatory authorities). Use of a consistent set of safety guidelines, ground rules, and objective safety analysis assists in ensuring that consistent decisions are made between product models and programs. Appendices K and L describe elements of manufacturer SB and AD processes, respectively.

If the decision made is to approve the proposed action(s), the process continues into the “DISPOSITION ACTION PLAN” phase and the “Prioritize & Schedule” and “Implement” steps begin.

If the recommended action is not approved by the organization, they must determine how to proceed. If more analysis is needed, then the process may return to either the “ASSESS EVENT AND RISK” step to reassess the significance of the recommended action, or to the “DEVELOP ACTIONS PLAN” step to refine potential action. If the recommended action is not organization approved and no further analysis is deemed necessary, the process moves to the “Document & Close” step. The decision and its justification are then documented and filed for future reference.

3.2.4.4 Action Applicability Review

The “Action Applicability Review” step is performed by the potentially impacted organization to determine if an externally created action (e.g., SB or AD) affects any airplane in their fleet.

Operators may receive externally developed actions in the form of service bulletins (SBs). Appendix J describes the operator process for handling SBs.

In the case of externally directed resolutions such as airworthiness directives (ADs), the basic action and implementation schedule will already be defined. For other resolutions, such as Alert Service Bulletins (ASBs), Service Bulletins (SBs), or Service Information Documents (SIDs), the basic action and implementation schedule will be suggested but will need to be factored into the operator’s overall implementation plan and prioritized. If the regulatory agency action or schedule cannot be met, the operator or manufacturer has the opportunity to request equivalent actions that provide the same level of safety. This forms the basis of the Alternative Means of Compliance (AMOC). The intent of the AMOC is to enable approval of options that were not necessarily conceived at the time of issuance of the original action, but that provide an equivalent level of safety to that afforded by the original action. The safety assessment process delineated in this document can be used to help determine if a proposed AMOC provides an equivalent level of safety. Appendix L discusses the regulatory AD process in more detail.

When the external action has been created to resolve an issue identified by the reviewing organization earlier, it should be carefully reviewed by the appropriate technical experts to ensure that it does in fact fully resolve that problem. Any concern with the proposed action should be communicated to the external party as soon as possible.

In cases other than ADs, a study to determine the costs and benefits may be performed. If the decision is to implement, the process continues to “DISPOSITION ACTION PLAN” phase and the “Prioritize & Schedule” and “Implement” steps begin. If the decision is to not implement the action, the process moves to the “Document & Close” step. The decision and its justification are then documented and filed for future reference.

3.2.5 Disposition Action Plan

The “DISPOSITION ACTION PLAN” phase is composed of the “Prioritize & Schedule,” “Implement,” “Actions to Other Levels,” and “Document & Close” steps.

3.2.5.1 Prioritize & Schedule

“Schedule” is unique to each organization and depicts their specific processes and approval cycles. The combined effects of hazard, probability of occurrence, risk exposure, and availability of parts and other resources assist in determining the priorities to implement the actions. During the normal execution of the process, several potential problems may be evaluated at the same time. This usually results in the need to prioritize the order in which problems will be corrected. The process encompasses determining relative priorities (e.g., risk reduction, cost, ease of implementation) of this and other actions and scheduling implementation.

This step may involve the scheduling of tasks and resources required to create and issue a service bulletin and to organize the availability of parts, etc., that will be required by the operators. If the affected airplane design is in production, the airplane manufacturer will also need to determine the production introduction of the corrected design. For an operator, this step may involve the scheduling required to incorporate an actual design change into airplanes in their fleet, or incorporate changes into their maintenance or operational programs.

The final aspect of this step is to establish a complete and coordinated implementation plan. Some simple action implementations may have very straightforward, simple, and non-time critical implementation plans. Other actions may require coordination of specific airplane changes combined with crew or maintenance procedure change requirements or training resulting in more complicated implementation plans.

Once an applicable implementation plan is developed and organizationally approved, actual implementation is initiated.

3.2.5.2 Implement

When the action plan is defined and verified to appropriately resolve the problem or concern, it can be implemented into the fleet or organization. Problem resolutions should be monitored for effectiveness to ensure that the action was effective in reducing or eliminating the problem. The monitor performance criteria and method of gathering and assessing the data should be defined within the “DISPOSITION ACTION PLAN” phase and forwarded to the “MONITOR FOR EVENTS” phase. If this monitoring determines the action is not effective, the problem reenters the ongoing safety assessment process, where additional data gathering and root cause analysis may be necessary. Re-addressing of the problem then continues through the normal safety assessment process, leading to revised action plans and implementations.

Verification and validation of the problem resolution should be an integral part of this step. Refer to ARP4754 for guidance in this area.

Unacceptable delays in the availability of the final action plan may necessitate development of an interim mitigating strategy such as an inspection program or modified operating procedures until the final action plan can be incorporated.

Although not always available in current practice, a closed-loop process is preferable; i.e., implementation should be carefully monitored to track completeness of the implementation process at any given time. This is particularly important in addressing ADs, manufacturer-required changes, or operator-driven changes, where knowledge of the status of percent of fleet addressed to date may be beneficial.

Throughout the process for any one potential problem, it is possible that new insight to “Establish Expectations” or “Establish Monitor Parameters” steps may arise. In these cases, the experience gained and lessons learned should be carried back into these steps and appropriate modifications put in place within the continuously operating portion of the assessment process. This iterative process improvement benefits effectiveness of the process for any specific user implementation.

3.2.5.3 Actions to Other Levels

Forward SBs, ADs, or proposed actions to other organizations that may also be affected for consideration of implementation. Some manufacturers have contractual agreements with operators for SB implementation tracking while others do not.

3.2.5.4 Document & Close

Normally, a problem resolution will be implemented through the issuance of an official technical document from the organization implementing the change. Examples of documents which may be changed include:

- a. Flight Operations Manual
- b. Engineering Orders
- c. Maintenance Alerts
- d. Maintenance Manuals
- e. Flight Operations Bulletins

For a manufacturer, the document issued may:

- a. Be focused toward the operator in the form of a Service Bulletin, Service Letter, All Operator Telex, Maintenance Tips, etc.
- b. Be directed toward its own organization, which may include new process instructions, production guidelines, new drawings, etc.

The regulatory agencies may issue an AD to ensure compliance with actions that are deemed mandatory.

In most cases, the document used to implement the change within the organization becomes the means for documenting closure of the project. In other cases, the organization may maintain a running log of all the problems in process and may update that log to show how the problem was resolved and which documents were used to close the issue, including those problems for which no action was taken.

In many cases, simply issuing a document will not resolve the problem. It is the response to the issued document by production, design, training, maintenance, or flight personnel that resolves the problems. Thus, the initial document used to implement the change may create a series of documents that must be acted upon. In many cases, new processes will be published, training programs will be developed, and, finally, personnel will be trained to act in a way that will resolve the problem. Continued monitoring may be required to ensure all processes, modifications, and training have been effective.

Assuming the series of documents, processes, and modifications have been accomplished and monitoring shows that they have successfully resolved the problem, the organization will then go back into a mode of monitoring parameters and perhaps evaluating lessons learned from the resolution process.

If no action was taken for the event, the decision and rationale are preserved in the Document & Close step.

3.2.6 Lessons Learned

The objective of a Lessons Learned process is to use in-service experience to improve all aspects of airplane operations and design. The introduction of a Lessons Learned process enables a systematic reuse of factual experience in an efficient way so that performance characteristics, such as the following, may be improved:

- a. Safety, reliability, availability, maintainability, cost
- b. Quality of products as well as quality of the company processes
- c. Number and cost of modifications of the products
- d. Compatibility of human/machine interface
- e. Satisfaction of users' needs

Appendix N presents a detailed discussion of the Lessons Learned process and the elements needed to make it successful.

3.3 The Integrated Ongoing Safety Assessment

A detailed, integrated industry flow chart is shown in Figure 4. Depending on the types of problems under consideration and decided depth of the ongoing safety assessment process, not all steps described above in 3.2 may be needed.

There are several users of the process described in the previous sections:

- a. Operator
- b. Airframe manufacturer
- c. Supplier
- d. Airworthiness authority

Each user incorporates the set of processes applicable to them. Figure 4 depicts three interactive processes and the communication flow among them. While the processes are similar for each type of user, the activities vary due to differences in the types of information available and considered, and the requirements and expectations. For example, an operator may have a different outlook regarding an in service event than that of the airframe manufacturer or an equipment supplier. The airframe manufacturer may refer to information not readily available to the operator or supplier (e.g., fault trees and/or FMEAs done during development).

Operators, airframe manufacturers, suppliers and airworthiness authorities may receive event notifications from their own monitoring or from other organizations. For example, when an operator recognizes a problem related to a specific supplier product, the operator process "Internal/External Action?" decision in Figure 2 identifies the action as not being an operator issue. The operator should contact the airframe manufacturer, or supplier, advising them of the problem. This identifies the event as an input for the manufacturer or supplier "ASSESS EVENT & RISK" process phase. The problem should be delegated to the responsible organization through the manufacturer and/or supplier processes, and that organization should develop the action. When the action is developed and organizationally approved, the action is given (by AD, SB, etc.) to operators and manufacturers as an input to a potential "Action Applicability Review" step.

The example above identifies three users (operator, manufacturer, and supplier). Parallel implementations of the processes also exist. One operator may detect a problem and advise other operators, or the airframe manufacturer and supplier working the issue may advise other operators. Similar instances may occur with multiple airframe manufacturers or suppliers, leading to a matrix of possible interactions.

There is also a fourth parallel path being executed by the regulatory authorities. This path results in airworthiness directives. In general, the Airworthiness Directive (AD) process is similar to the Ongoing Safety Assessment Process shown in Figure 2. The details in the AD process vary due to differences in the types of AD actions considered. Depending on the types of the problems under consideration and on the decided depth of the AD process, not all steps shown in Figure 2 may be required. The AD process and its regulatory elements, the coordination flow among the authority, manufacturers, suppliers and operators are discussed in detail in Appendix L.

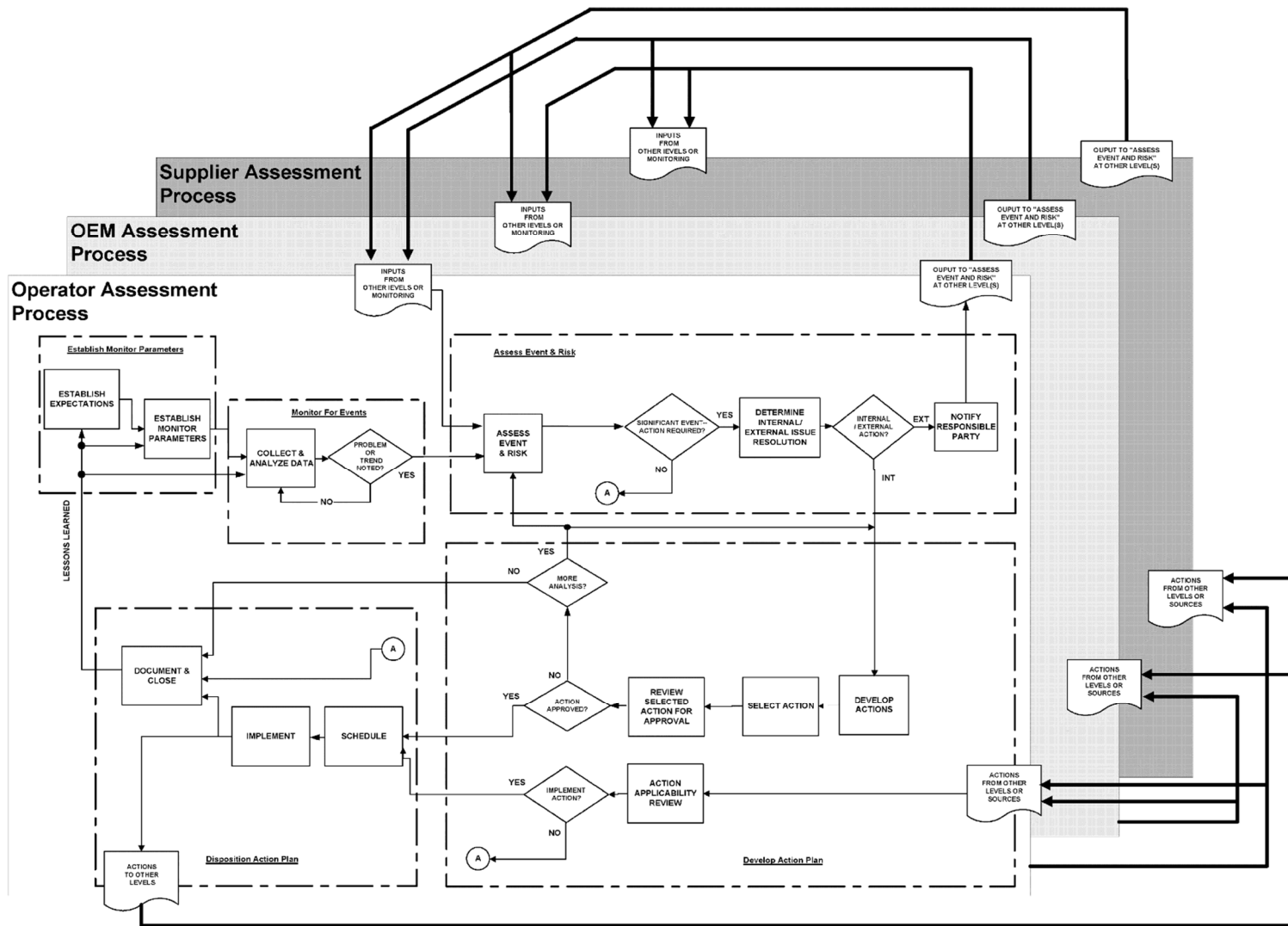


Figure 4 - Integrated ongoing safety assessment process

3.4 Related Topics

The following sub-sections describe independent topics related to the safety assessment process.

3.4.1 Review of Process and Organization Effectiveness

It is recommended that the ongoing safety assessment process include independent safety review practices as an integral part of the safety assessment process conducted by the organization. These reviews may be accomplished either internal or external to the organization. These reviews address the following two questions:

1. Is the organization following the safety assessment process?
2. How effective has the safety assessment process been?

3.4.2 Alternative Dispatch Conditions

The regulatory authorities require that all equipment installed on an airplane in compliance with the Airworthiness Standards (e.g., 14 CFR Parts 121, 135) and the Operating Rules (e.g., 14 CFR Parts 91, 121) must be operative. Experience has proven that, due to the various levels of redundancy designed into an airplane, operation of every system or installed component may not be necessary when the remaining operative equipment satisfies the airworthiness authorities. Therefore, certain conditional deviations from the original requirement are authorized to permit airplane dispatch. These "Dispatch Deviations" identify what is required to operate the airplane in the various non-standard configurations allowed by the type certification authorities-approved Master Minimum Equipment List (MMEL) and Configuration Deviation List (CDL), and by the operations regulatory authorities-approved Minimum Equipment List (MEL).

3.4.3 Design Changes

Where design changes have been made as a result of the safety assessment process, or for other safety-related reasons, it is reasonable to assume that consideration of safety impact has been made. However, there are other reasons for design changes, including producibility, functionality, or cost effectiveness. These should be reviewed for safety impact.

Dealing with these issues can be difficult, as there is frequently no single point or organization that controls the use of components. The most common processes here are likely to be training and awareness of potential issues by operator's procurement and maintenance personnel. The magnitude of the task may be reduced through identification of safety-related functions, products or components. With this identification in place, functions, products or components not identified may generally be excluded from any detailed safety review.

As an example, the primary hydraulic actuators, flight control computers, primary display systems, and engines and their controls frequently qualify as safety-related items and are subject to monitoring, while passenger entertainment and galley equipment may not require further monitoring.

The change categories addressed in this section include non-safety-related design changes, changes due to obsolete or non-procurable parts, and possible use of "counterfeit" or non-traceable parts.

3.4.3.1 Safety Impact of Non-Safety Design Changes

Design changes may be initiated in safety-related equipment to increase productivity, reduce cost, increase interchangeability, or various other reasons. These changes may be initiated by well-intentioned employees for very good reasons; however, those employees may be unaware of safety-related issues associated with the designs. Every change to safety-related equipment should be carefully reviewed by an engineer familiar with the function of the component, its safety implications, and, where possible, why it was initially designed the way it was. Examples of changes that may appear acceptable but may have adverse safety impact may include:

- a. Differences in surface machining or finish plating (e.g., servo slip clutches, components exposed to corrosive environments)
- b. Differences in form factors (some servo housings are intentionally non-symmetrical to preclude incorrect installation of critical parts where incorrect assembly may be difficult to detect and hazardous)

- c. Mechanical or electrical limitations of a component affecting operational characteristics
- d. Cable, tubing, or wire sized for non-standard forces or flows required for emergency situations, but apparently “excessively sized” for normal operation
- e. Changes in wiring that invalidate wire separation
- f. Changes to the finish on composite components

3.4.4 Alternative Parts

3.4.4.1 Substitution for Obsolete or Unavailable Parts

With today's technology and production processes, many parts that were in common usage and production in the past are becoming difficult or impossible to acquire. When parts used in safety-related products become unprocureable, substitute or alternative parts meeting all original requirements and qualifications will be identified, or products will be re-designed or re-certified with alternate parts incorporation.

When investigating alternative parts acquisition, the user should contact the original component manufacturer to identify qualified replacement parts whenever possible. Where this is not possible, the user should acquire the procurement specification of the original equipment parts and obtain assurance from potential replacement suppliers that their parts comply with the original specification, or identify specific areas of non-conformity. These areas of non-conformity should be carefully analyzed to determine if the differences will have a safety impact on the overall operation in all anticipated operating conditions and environments.

When components compliant with all of the original component specifications cannot be located, installation of parts that are non-compliant in a product, may cause the operation of the product to perform outside the limits of product certification. In some cases, analysis may identify these areas; in other cases, repeating some of the original certification testing may be required.

In many cases, the original equipment manufacturer (OEM) may have already generated service bulletin or modification recommendations to address the issue of unavailable parts. The manufacturer may also be able to provide information on the safety impact of certain replacement parts.

3.4.4.2 Counterfeit Parts

The expense and difficulty in obtaining qualified replacement parts for safety-related equipment has resulted in a black market of uncertified, uncertifiable, or counterfeit parts. In some cases, this is unintentional and the parts may meet the necessary qualifications but their compliance may not be verifiable and traceable. In other cases, the parts are intentionally misrepresented by opportunistic suppliers.

One approach to assuring that counterfeit parts are not introduced into the fleet is through training of procurement, supervisory, parts administration, and line maintenance personnel. This training should describe the issues and concerns, especially safety, and recommend that procurement employees deal only with known reputable suppliers, require certification of component traceability to be delivered with components, and beware of “too good to be true” availability or part pricing.

Line maintenance and employees administering parts stocking and distribution should be on the lookout for any differences in parts they usually use, and forward these parts and an explanation of their concerns to the appropriate channels for confirmation of certificability of the parts prior to their incorporation in an airplane.

3.4.5 Safety Processes and Human Performance

Human performance is an area of much current interest and research in the aviation field. The topic spans the spectrum from the original design of the airplane to all aspects of its operation and maintenance. This document considers human performance only as it plays a role in the ongoing safety assessment for a specific scenario or problem under study; it does not attempt to include or summarize the current state of human performance research. However, the Ongoing Safety Assessment Process flow chart (Figure 2) describes a series of activities, tasks, and decisions that are as applicable to human performance as they are for more commonly discussed design and quality problems. These human performance considerations should be integrated into standard in-service event analysis processes and ongoing safety assessment processes.

3.4.6 Maintenance Program Development

The initial maintenance program for an airplane type is created using the Maintenance Steering Group-3 (MSG-3) process. This process contributes to the development of the Maintenance Review Board (MRB) document and Maintenance Planning Document (MPD) created by the manufacturers, operators, and regulators.

The MRB document contains the minimum maintenance requirements for the airframe, engine, and components for a given airplane. The MRB document is established in a series of working group meetings, consisting of engineers from the manufacturer, operators, vendors, and the regulatory authorities. Maintenance requirements are analyzed to determine what task is required and at what interval it is necessary to accomplish the task to ensure that the airplane will be maintained in a safe, reliable, and airworthy condition at a reasonable cost. The MRB document includes scheduled maintenance tasks developed as part of the design process, including certification maintenance requirement (CMRs) tasks.

The MPD or the On-Aircraft Maintenance Planning Document (OAMPD), as some manufacturers call their planning document, is derived from the MRB as well as other recommended maintenance tasks that have come from service bulletins (SBs) or service information letters (SILs). The tasks that have been created from the SBs and SILs are recommended tasks, which, if incorporated into an operator's maintenance program, should be an enhancement.

3.4.7 Process to Appendix Cross Reference

This section provides a handy cross-reference to summarize the significant appendix utilization by each ongoing safety assessment process step.

STEP 1: ESTABLISH MONITOR PARAMETERS:

APPENDIX N	LESSONS LEARNED
------------	-----------------

STEP 2: MONITOR FOR EVENTS:

APPENDIX H	FLIGHT OPERATIONAL QUALITY ASSURANCE (FOQA)
APPENDIX L	MAINTENANCE ERROR DECISION AID (MEDA)

STEP 3: ASSESS EVENTS AND RISK:

APPENDIX A	SAFETY SIGNIFICANT EVENT REFERENCE LISTS
APPENDIX B	QUALITATIVE RISK ASSESSMENT
APPENDIX C	QUANTITATIVE RISK ASSESSMENT
APPENDIX D	ROOT CAUSE (Event Tree) ANALYSIS
APPENDIX E	WEIBULL ANALYSIS
APPENDIX F	MONTE CARLO ANALYSIS
APPENDIX G	RELIABILITY GROWTH MODELING
APPENDIX M	HAZARD TRACKING

STEP 4: DEVELOP ACTION PLAN:

APPENDIX J	OPERATOR SERVICE BULLETIN PROCESS
APPENDIX K	MANUFACTURER SERVICE BULLETIN PROCESS
APPENDIX L	AIRWORTHINESS DIRECTIVE DEVELOPMENT PROCESS

STEP 5: DISPOSITION OF ACTION PLAN:

4. IN-SERVICE DATA

This section provides a review of data sources currently available, as well as a recommended framework for collection, analysis, and sharing. Where pertinent, limitations and strengths of the various data sources are also presented in Section 6, which provides a description of each data source as well as a contact point to assist in further definition.

4.1 The Systemic View of Safety Information

Vertical and horizontal integration of safety assessment programs improves the comprehensiveness of field data, assures correct assessment of risk severity, and reduces conflict between organizations. Within an organization, vertical integration promotes a culture of safety from the chief executive officer down to lowest-level employees, while horizontal integration facilitates collaboration and coordination across functional lines (e.g., maintenance, operations, safety). In the aviation industry as a whole, vertical integration encompasses all the organizations required for the airplane to be designed, approved, and safely operated (i.e., engineering/design, manufacturing, operations and maintenance, and regulatory oversight), while horizontal integration refers to collaboration, coordination, and sharing among equivalent functional areas across organizational lines (e.g., maintenance at airline “A” with maintenance at airline “B,” regulatory decision from country “A” with those from country “B”).

4.2 Categories of Data

A thorough safety assessment function requires the collection and analysis of many different categories of data. These range from official sources of data on accidents and incidents to voluntary event/incident reporting to daily operations summaries and reliability reporting. The following sub-sections provide an overview of the basic categories and sources of data. Table 1 identifies who generally has access to the various types of data. For a list of currently available and planned airplane safety-related data sources, see Section 6

4.2.1 Accident Data

Accident investigation is a vital part of safety assessment. Accident data contains safety information that can be used to prevent future severe events. There are two basic categories of accident data: official sources and unofficial sources.

In United States, the only official source of accident data on civil accidents is the National Transportation Safety Board, charged by the Independent Safety Board Act of 1974 with the investigation and reporting of all aviation accidents. The NTSB database contains all reported fatal and non-fatal accidents involving U.S.-registered airplanes and occurring within United States and its territories. All operational categories are included. While by law, all fatal and non-fatal civil aviation accidents must be investigated and reported on by the NTSB, it is important to understand the distinction between a full-blown “Go-Team” investigation of an air carrier accident and a typical general aviation accident. The “Go-Team” accident involves many teams and sub-teams and months of investigation, often involving complete reconstruction of the aircraft. On the other hand, the typical general aviation accident is investigated by a single individual from the FAA or the NTSB, and is usually completed within 24 hours.

To support the international community, ICAO maintains an official accident and incident database containing reports from its 186 member states submitted in accordance with Annex 13. Two important distinctions compared to the NTSB are: this database only contains accident information for aircraft that have a maximum gross takeoff weight in excess of 2250 kg, and, most importantly, the quality of the submitted report varies from member state to member state.

Many countries, such as the United Kingdom, Canada, France, Germany, and others, also maintain official accident report records for occurrences within their countries.

Other sources of accident information are other government agencies (e.g., FAA, NASA), manufacturers, insurance companies, aviation safety associations (e.g., Flight Safety Foundation (FSF)) and even aviation enthusiasts within the general public. Some are listed in Section 6, but they should be used with caution, particularly if their information differs from the official accident investigation report. A notable exception is Ascend, a very large insurance carrier that maintains its own database of accident information to settle claims. There are many cases where there is no official report of the accident, yet the Ascend database contains an “unofficial” report. The Ascend reports also frequently contain updated damage information beyond what the NTSB has.

Though typically not pertinent to civilian operations, each of the US military services maintains a database of its accidents. There are common aircraft makes and models, airspace, and airports, which can frequently yield useful information.

Table 1 - Database access

Data Base	Participant		
	Operator	Manufacturer	Regulatory Authority
Accident Data	√	√	√
Ascend	√\$	√\$	√\$
Incident Investigative Agency (ex. NTSB)	√	√	√
Airworthiness Regulatory Agency (FAA, EASA, etc)	√	√	√
Operator Incident Data			
- Reportable	√	√	√
- Non-Reportable	√*		
NTSB / Regulatory Authority Safety Recommendations	√	√	√
Safety Difficulty Reports	√	√	√
Airworthiness Directives Subsystem	√	√	√
Manufacturer data		√*	
Safety Information/Incident Reporting System	√*		
Daily Operational Summary	√*	√*	V +
Operator Reliability data	√*	√*	√ +

* Own data only. + Local authority only \$ Fee for service

4.2.2 Incident Data

Unlike accident data, incident data may provide information to develop actions before a severe event occurs.

In the United States, there are two primary sources for incident data, the NTSB and FAA. The NTSB maintains a record of all mandatory reporting incidents cited in 14 CFR Part 830, which includes fire in flight, uncontained engine failure, flight control system malfunction, and others. The FAA maintains a record of the incident reports in accordance with FAA Form 8020-5. This database contains a large number of entries on bird strikes, collisions with objects, collisions with other aircraft, component failures, tail strikes, and other events.

The FAA also operates a separate incident monitoring system that contains pilot deviations, operational errors, near mid-air collisions, vehicle/pedestrian deviations, and runway incursions.

Many of the FAA safety-related information systems are collected and made available through Aviation Safety Information Analysis and Sharing (ASIAS) System, the FAA focal point for collection and analysis of safety information.

An extensive database on incidents is also maintained by NASA. It consists of voluntary reports submitted by air crews and air traffic controllers, mechanics, and other interested parties, and it is unique in that it offers FAA violation immunity to the reporter.

The United Kingdom, Australia, Canada, and many other countries also maintain incident reporting databases.

Some of the most valuable sources of incident data, however, are aviation associations and individual operators. The Air Line Pilots Association (ALPA), Aircraft Owners and Pilots Association (AOPA), Flight Safety Foundation (FSF), Allied Pilots Association (APA), and many of the larger U.S. airlines all operate internal incident reporting systems. In the hierarchy of accidents, official incidents, and unofficial incidents, these internal incident reporting systems provide the greatest opportunity for improvement of aviation safety. They represent many minor and some major incidents that could evolve into an accident based upon the circumstances. Collaboration, coordination, and sharing of this incident information may provide the framework for a substantial improvement in safety assessment.

4.2.3 Safety Recommendation Data

The NTSB and FAA operate safety recommendation systems. The NTSB recommendations system contains the formal safety recommendations made to the FAA, the FAA's response, and final adjudication. The FAA safety recommendations system is operated by the Office of Accident Investigation and contains safety recommendations submitted by FAA field personnel.

4.2.4 Other Official Data

There are several other official sources of information pertinent to airplane safety assessment. These include the Service Difficulty Reporting System (SDRS), the Master Minimum Equipment Lists (MMEL) subsystem, the Airworthiness Directives (ADs) subsystem, and the Automated Federal Aviation Regulations (AFAR) subsystem.

The SDRS contains general aviation malfunction/defect reports and air carrier mechanical reliability data. The bulk of this information is submitted by air carriers and general aviation maintenance personnel.

The MMEL subsystem contains a complete list of required equipment and conditions under which each make and model of airplane operated by air carriers may operate. The MMEL Regulations are also included.

The Airworthiness Directive subsystem contains the full text of all airworthiness directives issued for all aircraft with U.S. registry. This system includes both current and archived ADs.

The AFAR subsystem contains the full text of all United States CFRs.

4.2.5 Data from Manufacturers

Fleet-wide information is available from OEMs. This includes service difficulty information, reliability information, service bulletins, and service letters. The key data information available from the manufacturers includes the airplane/systems design and production knowledge.

4.2.6 Operator-Level Data

4.2.6.1 Safety Information/Incident Reporting Systems

As the complexity of the safety assessment function has grown, many of the larger operators have installed sophisticated information systems, which link their organization vertically and horizontally for the sharing of information. With the proliferation of these systems, the distinction between safety information and other information is disappearing. More and more operators are experiencing the benefits of an information collection and feedback process. Much information that was thought to be only safety related in the past now yields other benefits such as lower operational costs. For example, a reliability monitoring program targeted at landing gear performance is capable of predicting a failure sufficiently in advance such that preventive maintenance can avoid both an incident or accident as well as the lost revenue associated with unscheduled downtime.

Accompanying these information systems are standards, policies and procedures related to the reporting, collection, analysis, and dissemination of safety-related information. There are several key attributes of the systems and their associated policies, which determine the effectiveness of the overall safety assessment program they govern. They are:

- a. Support and empowerment from organization executives
- b. Encouragement of voluntary, non-punitive reporting policies
- c. Vertical integration from lowest-level employee to the chief executive officer
- d. Horizontal sharing of information across functional lines within the organization
- e. Positive action and follow-up when problems are detected
- f. Constant feedback from all levels of the organization, both for necessary improvements and positive reward
- g. Requirements-based data collection and analysis; i.e., avoid collecting data for the sake of collecting data, have a purpose
- h. User-friendly applications programs to increase acceptance

There are various off-the-shelf safety information systems, such as the British Airways Safety Information Service (BASIS), which an organization can purchase or lease, thereby avoiding extensive development costs. These systems come with sufficient applications software to support data entry, analysis, communications, networking, and reporting to permit an organization to begin an immediate safety assessment program. Section 6 lists some off the shelf systems/services that currently exist.

4.2.6.2 Daily Operational Summary

The Daily Operational Summary typically consists of the previous day's flight data, on-time performance, canceled flights, diverted flights, operational difficulties with ATC, airports, weather, or other factors. The report may also detail any airplane ground damage, inflight emergencies, load errors, hazardous materials incidents. A summary of the out-of-service airplane may also be provided. This summary may detail specific maintenance requirements, status of work, total number of MEL/CDL items and other information as deemed necessary.

4.2.6.3 Air Carrier Reliability Data

Many carriers operate internal reliability programs. These programs have a positive impact on both safety and operations costs. Through continual monitoring and assessment of daily operations and maintenance, reliability trends (including re-occurrences) can be developed and monitored for exceptions. When exceptions occur, very often before an incident or accident occurs, preventive action may be taken to mitigate the impact on either safety or operations costs. Establishment of an effective reliability program requires collection and analysis of a breadth and depth of information. Examples include:

- a. FOQA (see Appendix I)
- b. Aircraft Maintenance Logs (Pilot Reports, Maintenance Discrepancies)
- c. Fleet Delays and Cancellations (e.g., Air Turnbacks, Diversions, Aborts, Repeats)
- d. MEL/CDL Deferrals
- e. Operational/Service Difficulty Reports (ODRs, SDRs)
- f. Engine Monitoring Data (Inflight Shutdowns, Removals)
- g. Component Maintenance Activity (Removals, Tear-Down Reports, History)
- h. Category I/II/III Landing Data
- i. Hangar Maintenance Discrepancies
- j. Corrosion Prevention Control Program (CPCP)
- k. Structural Sampling
- l. Supplemental Structural Inspections
- m. Hydraulic Gross Flow Check
- n. Flight Recorder Data
- o. Airplane Damages
- p. Flying Time/Cycles

The systematic collection of the types of data listed above and the use of this data in ongoing safety assessment, combined with the preventive action necessary will have a positive effect on both safety and operating costs.

5. METHODS AND TOOLS

The following sections provide brief descriptions of a number of assessment and analysis methods and tools available for use in a safety risk analysis (SRA).

Additional methods and tools, such as Markov Analysis, Fault Tree Analysis, Dependence Diagramming, Failure Mode and Effect Analysis, Common Mode Analysis, Zonal Safety Analysis, and Particular Risk Safety Analysis are identified and discussed in detail in ARP4761.

As described in FAA AC39-8, Continued Airworthiness Assessments of Powerplant and APU Installations of Transport Category Airplanes, any analysis is only as accurate as the assumptions, data, and analytical techniques it uses. Therefore, the underlying assumptions, data, and analytic techniques should be identified and justified to assure that the conclusions of the analysis are valid. Variability may be inherent in elements such as failure modes, failure effects, failure rates, failure probability distribution functions, failure exposure times, failure detection methods, fault independence, human interfaces (e.g., crew actions and procedures), and limitation of analytical methods, processes, and assumptions. The justification of the assumptions made with respect to the above items should be an integral part of the analysis. Assumptions can be verified by using experience with identical or similar systems or components with due allowance made for differences of design, duty cycle, and environment. Where it is not possible to fully justify the adequacy of the analysis and where data or assumptions are critical to the acceptability of the conclusion, extra conservatism should be built into either the analysis or the action. Alternatively, any uncertainty in the data and assumptions should be evaluated to the degree necessary to demonstrate that the analysis conclusions are insensitive to that uncertainty.

It is essential to identify and document any assumptions and uncertainties related to a safety analysis in order to be able to judge their effect on the conclusions of such an analysis and to conduct sensitivity analysis.

On-going field experience should be monitored to continue validation of the assumptions and to mitigate uncertainties, or to obtain the data necessary to alleviate any consequence of the extra conservatism built into the initial analysis. The finding of any shortfalls in the assumptions calls for consideration of revision to the SRA.

Furthermore, the necessity of calibrating the SRA with the past experience helps to ensure that the future prediction is reasonable, assuming that operational parameters (derate schedules, etc.) remain constant. If the analysis does not calibrate, there will need to be further review to determine which safety analysis assumptions may be in error. The SRA will not predict reliably if it cannot calibrate to the actual experience.

5.1 Root Cause (Event Tree) Analysis

Root Cause Analysis (RCA) is a method for establishing the potential root causes of a failure in an organized and thorough manner, providing full documentation of the investigation process. RCA utilizes an event tree, which is based on qualitative fault tree analysis, but shows only the cause-effect relationships of events without the use of logic gates. Potential root causes that may be contributors to the failure can be evaluated independently or in combination. Potential root causes include design deficiencies, crew errors, maintenance technician errors, operational manual deficiencies, etc. The final event tree and the root cause disposition process provide documentation and traceability to ensure thoroughness of the failure investigation.

Failure investigation is an essential tool in the development of various systems. When a failure occurs, an investigation team is assembled to determine the cause of the failure and make recommendations for action. Priority is assigned to the investigation based on how often the failure could potentially occur and how severe its effects may be. During the investigation, it must be determined how the failure is occurring, why it is occurring, and what needs to be done to adequately reduce the frequency or severity of the failure. In the case of failures that may result in potentially catastrophic events, these answers must be generated quickly so that the action can be implemented prior to another occurrence. In the past, this often resulted in a "quick fix" approach, in which a rapid decision was made as to the cause of the failure based on the single most credible scenario. A test program would then be set up to prove that the suspected sequence of events could cause the failure, and action would be proposed and demonstrated. Unfortunately, it was not uncommon for the failure to recur even after the action was implemented because the quick fix approach did not always identify all contributing causes of the failure. Thus, the process would begin another iteration, usually with more urgency and attention than the previous investigation. An approach similar to the fault tree can be used for failure investigations, where the top event on the fault tree is the undesired event (the failure under investigation). The main advantage of the fault tree process over the quick fix approach is that all plausible causes of the failure are investigated and documented, until one *or more* root causes are identified and confirmed as the main contributors to the failure. This way, more than one root cause can be addressed with action, thereby increasing the chances that the action would completely address the failure. This approach produces a thorough analysis of the failure mechanism, and the analyst can be satisfied that the investigation has been carried out in a thorough and organized manner. A standardized process, called "Root Cause Analysis," is defined in detail in Appendix D.

5.2 Weibull Analysis

Weibull analysis provides a tool to statistically analyze service experience data for a selected component. Its primary distinguishing feature is that it quantifies reliability (or risk of failure) as a function of the age of the product. This makes it an ideal tool predicting risk due to age-related failures. Weibull analysis can help assess whether a field recall is needed, and, if so, what the appropriate recall schedule should be. Weibull may also be used to calculate survivability rates to help establish warranty programs (when to replace).

Weibull analysis has many applications. Some typical applications include:

1. Assess the product service life corresponding to a specific risk level
2. Assess the probability of reaching a pre-established life goal
3. Identify the "aging" effect for the product; i.e., identify how the failure risk per hour changes as the product accumulates service time
4. Assess the impact of extending warranty coverage
5. Assess the impact of establishing or extending a scheduled maintenance period
6. Judge the system-level reliability benefit of correcting a specific observed failure mode

Weibull analysis is described in more detail in Appendix E.

5.3 Monte Carlo Simulation Analysis

Monte Carlo simulation is a versatile method of analyzing problems that are probabilistic in nature. The analysis involves defining a mathematical model of the system being studied and operating the model repeatedly in order to observe the range of system outcomes. The model typically involves several probabilistic input parameters, where the parameter values are defined by probability distributions. The model also defines how these input parameters combine with each other and with non-probabilistic parameters to produce specific potential system outcomes.

The inputs to an aviation safety model might include the failure distributions of contributing failure modes, reliability of fault monitoring and accommodation provisions, scheduled inspections and repair intervals, effectiveness of maintenance actions, effectiveness of crew actions, expected range of flight conditions, and other relevant factors. Although the output format of a Monte Carlo simulation is usually tailored to the specific problem being studied, a typical output would be a prediction of the number of hazardous events for the next year, five years, or until fleet retirement.

For fleet problems requiring a corrective action, the Monte Carlo method can be used to help judge the acceptability of various proposed corrective actions and implementation schedules. Corrective action input might take the form of proposed changes to equipment design, revised inspection or maintenance schedules, constraints on flight conditions, or similar mitigations. Likewise, implementation schedule changes can be modeled to judge the benefit of various accelerated schedules. To judge the effectiveness of the proposed corrective action and implementation schedule, the Monte Carlo output (e.g., number of hazardous events) is compared to the original analysis.

Monte Carlo simulation is a stochastic technique, meaning that the outcome is a probabilistic function of the inputs. The simulation typically involves hundreds, thousands, or even millions of “trials” of system operation. For each trial, a specific value for each input parameter is randomly selected from the specific probability function for that parameter. The “random” selection of each input value is accomplished through a random number generator, which is included in most computer programming languages or mathematical modeling software packages.

Details of performing a Monte Carlo Analysis are presented in Appendix F.

5.4 Corrective Action Scheduling

The FAA uses quantitative risk analysis to establish the upper limit on the length of time that can be tolerated to correct an unsafe condition. Additional information on this is contained in Appendix O. Knowing the tolerable upper limit to a corrective action schedule is necessary information to ensure the corrective action schedule does not exceed allowable guidelines. However, a qualitative assessment is also needed to satisfy the principle that the risk from an unsafe condition should be mitigated as soon as it is reasonably practicable to do so, which is typically sooner than the upper limit given regularly scheduled maintenance intervals. These two considerations comprise the corrective action scheduling process; the quantitative risk analysis to determine the schedule upper limit, and the qualitative assessment to satisfy correcting the condition at the earliest reasonable opportunity. For unsafe conditions, the corrective action schedule will become mandatory through the AD process. Additional information on this is contained in Appendix L.

Not all corrective actions address an unsafe condition. Some issues might not be unsafe, but may still benefit from safety enhancement or product improvement modifications. In these cases, there is latitude in setting a recommended schedule for accomplishing the changes.

5.5 Sensitivity Analysis

Sensitivity analysis evaluates the effect of changes to the SRA input parameters on the results. Sensitivity Analysis also allows the analyst to assess the effects of variation in the major assumptions used in the analysis. Acquiring additional data on the analysis inputs will reduce the uncertainty and, therefore, reduce the range of possible results.

Some methods for providing justification of analysis assumptions are described in detail in ARP4761.

5.6 Reliability Growth Modeling

Reliability Growth Modeling is a graphical tool used to depict trends in the reliability of a product or system. Plotting various cumulative reliability parameters (e.g., cumulative events, cumulative failure rate, MTBF) versus a cumulative time function (e.g., hours, cycles) using a Crow-AMSAA or similar reliability growth model can provide insight into whether the reliability is improving or not, and by how much. Equations derived from the plots can be used to project the number and rate of future events and determine whether desired goals can be met.

Reliability Growth Modeling can be used to assess the positive results of improvements in product design, manufacture, or maintenance practices. It also can signal when mitigating action might be required due to an adverse condition or trend.

Details of performing Reliability Growth Modeling are presented in Appendix G.

5.7 Human Factors Methods and Tools

There are tools used for improvement of performance for flight and ground crews in an organization. Two of the more common tools are discussed in the following paragraphs.

5.7.1 FOQA

Flight Operational Quality Assurance (FOQA) is a voluntary program designed to improve aviation safety through the analysis of recorded digital flight data. Since 2006, commercial airlines have used this data to identify and correct deficiencies in all areas of their flight operations, thereby mitigating hazards to safety. Aggregate flight data is also analyzed and sanitized by an external entity and shared with the FAA under memoranda of understanding (MOAs). This allows the assessment of industry-wide trends and targets resources to reduce operational risks in the National Airspace System (NAS). The ultimate objective of a FOQA program is to identify lower-level safety trends in flight operations so that mitigation strategies can be implemented before a higher-level accident or incident occurs. The FOQA system is unique in that it provides insight into objective data that is not available through any other method. Further information on FOQA is available in Appendix H.

5.7.2 MEDA Tool

Maintenance and inspection errors have had serious safety consequences for the aviation industry. A review of airline data for the period of 1982 to 1993 suggests that maintenance and inspection errors are the primary cause of about 6% of the accidents and are a contributing factor in approximately 15% of the accidents. In addition, maintenance and inspection errors can have large monetary consequences to the airplane operator.

The Maintenance Error Decision Aid (MEDA) is a tool developed and distributed by Boeing without charge. It is used to assist in the resolution of maintenance error problems by providing a systematic checklist, which allows the investigator to collect sufficient information to arrive at a complete solution for a given problem. Once a series of events has been investigated, a database exists to aid the investigator on future event resolution. Further information on MEDA is available in Appendix I.

5.8 Fleet Risk Exposure Analysis

Fleet Risk Exposure Analysis is the use of probability analysis to determine the expected number of undesired events of a specific type in a given fleet based on the predicted or historical event or malfunction rate per flight and the actual or expected number of fleet operations (exposure). A graphical presentation of the results can assist in estimation of the probability of occurrence of the event under consideration, and the relative effectiveness of proposed actions, as fleet operations continue. A detailed description is contained in Appendix C.

6. BEING INVOLVED IN THE AVIATION SAFETY COMMUNITY

The sharing of safety information has become a high-profile issue in the aviation community. Sharing of safety data permits a more complete understanding of an issue than might be possible in isolation. It may not be possible to accomplish a complete evaluation without knowledge of problems that have been experienced by others operating the same airplane type. Even sharing with a select few other airlines, a common practice today, is not as effective as determining whether the whole community may have experienced similar problems. Current initiatives, such as the Global Aviation Information Network (GAIN) and the Aviation Safety Information Analysis and Sharing (ASIAS) system, have developed and implemented the means for sharing learned experiences across the industry for common good.

There are some conferences where safety is the main topic and numerous others where it is a subject of discussion. These conferences are opportunities for the safety engineer to talk with industry counterparts and establish contacts. These contacts can provide invaluable assistance in improving operations. Attending conferences is an effective way to expand one's knowledge of the latest safety advances in the participating organizations. The internet provides a convenient tool for finding lists of upcoming aviation safety-related conferences. Some safety-related conferences available at the time of publication are listed in Table 2.

Table 2 - Safety related conferences

Name	Purpose	Location	Date
Advances in Aviation Safety Conference	Conference dedicated to advancing safety knowledge in the industry.	Various USA	Spring
Annual International Air Safety Seminar	Joint meeting of the Flight Safety Foundation, International Federation of Airworthiness and International Air Transport Association held annually in selected cities of the world to ensure contact with the international aviation community.	Varies	Winter
Aviation Safety InfoShare	InfoShare is a confidential biannual conference sponsored by the FAA, in which Government and industry representatives share aviation safety concerns and discuss aviation safety issues and mitigations. Note: By participating in InfoShare, air carriers can fulfill the Title 14, Code of Federal Regulations § 13.401 requirement for disclosing FOQA data.	Various locations within the USA	Biannually
Flight Safety Foundation Annual Business Aviation Safety Seminar	Formerly the Corporate Aviation Safety Seminar, the Business Aviation Safety Summit is recognized as the premier forum for the discussion and exchange of safety information for corporate and business aviation operators.	USA	Spring
Flight Safety Foundation Annual European Aviation Safety Seminar (EASS)	Similar in format to the IASS, but focuses on safety challenges of interest to the European aviation industry.	Europe	Spring
Flight Safety Foundation Annual International Aviation Safety Summit (IASS)	The summit covers safety, training, practical solutions, management, human factors and other issues for scheduled airlines, manufacturers and equipment suppliers, trainers, flight crews, maintenance personnel and industry executives.	Various locations worldwide	Autumn

Name	Purpose	Location	Date
Global Aviation Safety and Security Conference	Annual Aviation Week conference of managers from international airlines and airports, policy makers, airworthiness authorities, equipment suppliers and researchers.	Washington, DC	Autumn
ICAO Accident Prevention and Safety Seminar	Conference of Govt. and private sector aviation officials.	Varies	Spring
ICAO Seminar on Accident Investigation, Prevention, and Human Factors		South America	Summer
International Society of Accident Safety Investigators (ISASI) Seminar	"Pushing the Envelope Towards Improvement."	Europe	Autumn
"Policies, economics, and Technology R&D for Aviation Safety"	Conference sponsored by the American Institute of Aeronautics and Astronautics.	Washington, DC	Spring
SMS Industry Forum	The SMS Industry Forum is a collaborative effort of industry lessons learned while creating SMS for their respective organizations and includes best practices.	Various USA	Spring
The Americas Conference on Aviation	Conference of U.S. Govt., industry, and aviation leadership from Latin America and the Caribbean. Conference themes are aviation safety, systems integration and training.	USA	Autumn
World Aviation Congress	Large gathering of aviation personalities and managers. Usually a session on aircraft safety.	Various USA	Autumn

Many websites have been established for the dissemination of safety information. Some of these are ready references for general safety data, and some provide detailed data on accidents and incidents. Website addresses change frequently; however, some of the websites available at the time of publication are listed in Table 3. Internet search results will yield many resources that discuss aviation safety-related topics. Search for "aviation safety," "aviation safety statistics," "aircraft accidents and incidents," or similar terms for updated information.

Table 3 below provides a list of commonly accessed websites for obtaining aviation-related safety data, and includes the website name, website address, and a brief explanation of the website's purpose and contents. Information in this table may be used in conjunction with Table 2, which provides a description of data sources, as well as a contact point to assist in further definition.

Table 3 - Safety related websites

Name	Address	Purpose
Aerospace Industry of America (AIA)	http://www.aia-aerospace.org/	Contains manufacturer related safety information.
Airlines for America (A4A)	http://airlines.org/	Provides publication list which can be ordered, good airline information handbook, links to airlines, government agencies.
Australian Transport Safety Board (ATSB) Aviation	http://www.atsb.gov.au/aviation/	ATSB Aviation Safety webpage.
Aviation Safety Information System of CAAC	http://safety.caac.gov.cn/	System Contains Aviation Safety Dynamic, International Aircraft Accident, International Safety information, Aviation safety audit information, etc.
Aviation Safety Network	https://aviation-safety.net	A service of Flight Safety Foundation, includes aviation safety database, accident investigation reports and accident statistics.
Civil Aviation Administration of China (CAAC)	http://www.caac.gov.cn/	CAAC Official website that contains CAAC regulations, Advisory Circulars, Aviation Procedures, etc.
CAAC Airworthiness Directive System	http://new.caacaa.org.cn/	System contains CAAC Airworthiness Directives, Biweekly report of CAAC Airworthiness Directives, etc.
Civil Aerospace Medical Institute (CAMI)	https://www.faa.gov/about/office_org/headquarters_offices/av/office_of_medical_and_safety_investigation/aam/cami/	FAA's Civil Aerospace Medical Institute site with links to information on Medical Bulletins, Industry testing programs, Medical certification, Pilots information and more.
European Aviation Safety Agency	https://www.easa.europa.eu/	EASA's main site containing agency information, links to EASA regulations, Agency rules, and a document library.
FAA Accident & Incident Data	https://www.faa.gov/data_research/accident_incident/	Full listing of accidents involving major airlines from 1920 to present, reports of recent accidents, sound files of CVR transcripts.
FAA Aviation Safety Information Analysis and Sharing (ASIAS) System	http://www.asias.faa.gov/	Integrated queries across multiple aviation safety databases; lessons learned from aviation accidents.
FAA Regulatory and Guidance Library	www.faa.gov	A variety of aviation safety information including 14CFR Parts 5, 21, 23, 25, 27, 29, 31, 33, 34, 35, 36, NPRMs, ACs, AD NPRMs and Final Rules, TCDS, Policy, Issue Papers, Special Conditions, Exemptions, Orders, TSOs, STCs, PMAs TARAM Handbook.

Name	Address	Purpose
FAA Engine & Propeller Directorate Technical Reports	https://www.faa.gov/aircraft/air_cert/design_approvals/engine_prop/engine_sp_topics/	Provides links to various technical reports containing propulsion system data, including the various CAAM Reports summarizing rates and outcomes of various engine, propeller and APU occurrences.
Flight Safety Foundation	http://www.flightsafety.org	Contains links to a number of aviation safety resources relevant to all aspects of aviation.
Global Aviation Safety Network	http://flightsafety.org/archives-and-resources/global-aviation-safety-network-gain	Information on GAIN Action Plan, Working Groups, Government Support Team and GAIN Conferences.
International Civil Aviation Organization (ICAO)	http://www.icao.int	About ICAO.
NASA Aviation Safety Reporting System	http://asrs.arc.nasa.gov/	Contains a description of ASRS program, recent ASRS publications, general reporting form as well as special forms for air traffic controllers, mechanics, and cabin crew.
National Transportation Safety Board (NTSB)	http://www.nts.gov	NTSB recommendations, publications, news, & events.
NTSB Aviation Accident Database	http://www.nts.gov/layouts/nts.aviation/index.aspx	Contains over 37000 accident and incidents descriptions involving U.S. aircraft or non-U.S. aircraft in U.S. jurisdiction and which occurred from 1983 to present.
SAE International - Aerospace	http://www.sae.org/aerospace	SAE Aerospace site with links to articles, events, publications and training related to the aerospace industry.
SAE International - Standards	http://www.sae.org/standards/	SAE S-18 standards development activities.
SKYbrary	http://www.skybrary.aero	SKYbrary is a wiki created and maintained by the European Organization for the Safety of Air Navigation, International Civil Aviation Organization, and the Flight Safety Foundation to provide a comprehensive source of aviation safety information.
The Royal Aeronautical Society	http://aerosociety.com/	Dedicated to global aerospace community, the Royal Aeronautical Society, also known as the RAeS, is a British multidisciplinary professional institution dedicated to the global aerospace community. It is the oldest aeronautical society in the world.
Transport Canada	www.tc.gc.ca	Include the Canadian Aviation Regulation Advisory Council (CARAC) and CARs regulatory information.
Transportation Safety Board (Canada)	http://bst-tsb.gc.ca	Transportation Safety Board (Canada) recommendations, publications, news, & events.
United Kingdom	https://www.gov.uk/government/organisations/air-accidents-investigation-branch	UK aviation accident investigation recommendations, publications, news, & events.

7. NOTES

7.1 Revision Indicator

A change bar (|) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY S-18C ARP5150A AND ARP5151A WORKING GROUP

APPENDIX A - SAFETY SIGNIFICANT EVENT REFERENCE LIST

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the body of the document.

A.1 SCOPE

The objective of this appendix is to provide sample lists of safety significant parameters for aircraft for which may be used for monitoring purposes or to enhance present and future aircraft designs.

These samples are intended to be example lists and not inclusive or prescriptive checklists since they may not include all the information necessary for appropriate failure conditions of an aircraft with its various functions and its intended use. It should be emphasized again that these sample lists of significant failure conditions examples should not be applied indiscriminately to a particular aircraft type and configuration.

This appendix has four sample lists - two from the view point of aircraft manufacturers, one from the perspective of an airline, and finally a cross reference list between one of the aircraft manufacturer lists and the airline list:

Table A1 - Aircraft Manufacturers Significant Failures List

Table A2 - Aircraft Manufacturers Failure Condition by System List

Table A3 - Airline Classification List

Table A4 - Significant Failure Conditions to Airline Significant Event Cross-Reference

To facilitate comparisons of design expectations and operational performance, it may be beneficial to monitor "lower level" parameters. In some cases, the objective may be to support compliance with the significant failure condition expectations.

A.2 AIRCRAFT MANUFACTURERS SIGNIFICANT FAILURES/ITEMS LIST BY FUNCTION EXAMPLE

Table A1 - Aircraft manufacturers significant failures list example

Function	ATA	Significant Failure/Item
Avionics	24	Any flight anomalies cause by Portable Electrical Devices (PED)
Avionics	23	Loss of Comm.
Avionics	31	Loss of Displays/Control Display Anomalies
Avionics	34	Loss of Nav. or Navigation Anomalies - FMF or sensor failures
Avionics	31/34	CDU Anomalies
Avionics	39	Configuration Problems (Incompatible HW/HW, SW/ HW) in a system
Avionics	31/50	Failure to warn/False Warnings (T/O Config, Land Config, GPWS, etc.)
Avionics	34	ARINC 629 Bus Failures
Avionics	02	Lightning Strike events
Avionics	22	Uncommanded Autothrottle Input
Avionics	34/10	Loss or Misleading Data from ADIRS or ADIRU
Doors	52	Cargo/Pax door EICAS messages
Doors	52	PED Flight Lock Failures
Doors	52	PED locked on ground
Doors	52	Passenger and Cargo door not fully closed, Latched and locked for T/O or LND
Doors	52	Pass. and Cargo door T/O Configuration Warning
ECS	36	Avionics equipment overheat
ECS	36	Cabin altitude warning/excessive cabin altitude/Loss of pressure control
ECS	36	Cargo fire extinguisher discharge
ECS	36	Cargo Fire Warnings

Function	ATA	Significant Failure/Item
ECS	36	Dual air condition pack loss
ECS	36	Duct burst events
ECS	36	Duct overheat events
ECS	36	Loss of auto cabin pressure control
ECS	36	Loss of equipment cooling - with no warning
ECS	36	Uncontrollable/excessive cabin temp
ECS	36	Use of equipment cooling override mode
Electrical	24	Degrading of wire shielding (Lightning and HIRF protection)
Electrical	24	Electrical smoke or fires
Electrical	24/27	Flight Control direct current (FCDC) system anomalies
Electrical	24	Loss of any IDG during turbulence, zero or negative Gs
Electrical	24	Main Battery Failures
Electrical	24	Power up problems in flight /Load shedding
Electrical	24/29	Failure of RAT Deployment/Inadvertent RAT Deployment
Electrical	24	Wire bundle chaffing (All Areas)
Flight Cont.	27	ACE logic for mode switching (Blocking/Bypass) (PFC Selection) (Direct)
Flight Cont.	27	Controllability with any Hydraulic and/or Electrical power losses
Flight Cont.	27	Control available versus. control required
Flight Cont.	27	Direct mode operations (Time and numbers of events)
Flight Cont.	27	Failure rates of the individual and or multiple PFC events
Flight Cont.	27	In direct mode any problems with dutch rolls or rudder structure damage
Flight Cont.	27	Loss or limited rudder control
Flight Cont.	27	Jams or restrictions of flight controls surfaces and controls
Flight Cont.	27	Secondary Mode Operation (Time and number of events)
Flight Cont.	22	Uncommanded AFDS input to the PFCS
Flight Cont.	27	Uncommanded surface movement
Flight Cont.	27	Use of PFC Disconnect switch (Time and number of events)
Flight Deck	3910	Confusion with Controls/Displays/Switches
Flight Deck	31/33	Lighting Failures
Flight Deck	52	No. 2 Window opening events on Takeoff which causes unnecessary RTOs
Flight Deck	25	Uncommanded crew seat movement
Flight Deck	02	Unplanned RTO - Reason for/ Speed
Mech System	32	Tire Burst/Failure Events: During T/O / LND / Taxi
Mech System	32	Brake Failure Events
Mech System	32	Main Gear Steering Events
Mech System	32	Nose Gear Steering Events
Mech System	32	Tire Burst/Failure Events: In Wheel Well During Flight
High Lift	27	Failure of load relief
High Lift	27	Flap/Slat Asymmetry Events In flight
High Lift	27	Flap/Slat Shutdown during cruise resulting in landing without flaps/Slats
Hydraulic	29	Anomalous low quantity indications on center hydraulic reservoir CHIS
Hydraulic	29	Chaffing of any hydraulic tubes near any ECS ducts - Mist in cabin
Hydraulic	29	Hydraulic System Loss (Single or Multiple)
Landing Gear	31	Inadvertent/Uncommanded gear extension
Landing Gear	31	Main gear tilt sequence anomalies
Landing Gear	31	Unsafe gear indication (Not down/Locked)
Landing Gear	31	Wheel well fire warning events - In flight or on ground
Payloads	38	Clear ice events
Payloads	52	Evacuation Conducted - Slide operation, etc.
Payloads	38	Lavatory flooding events - Flooding results with E/E Bay

Function	ATA	Significant Failure/Item
Payloads	35	Oxygen Events - Deployment failures, Loss of systems, O2 fires, etc.
Payloads	02	Personnel Injury Events - Cabin Interior Furnishings
Payloads	38	Potable water leaks
Propulsion	4910	APU Uncontained Failures
Propulsion	54	Burst duct events (Engine & Strut areas)
Propulsion	5430	Cowl hold open Rods failures
Propulsion	5440	Cowl Fairing separation events
Propulsion	72	Cross Engine Debris
Propulsion	72	Engine Compressor Stall: Engine Start in Tail Winds/Cross Winds
Propulsion	72/26	Engine Fires
Propulsion	7210	Engine Flame-outs/Roll-Backs/Sub-Idle (EFA Performance)
Propulsion	77	Engine indication anomalies
Propulsion	80	Engine Inflight Starts during revenue service
Propulsion	02	Engine personnel ingestion events
Propulsion	7120	Engine/Strut Mount problems
Propulsion	2840	FQIS Reliability versus. FMC Indications
Propulsion	2820	Firewall Shut-off Valve failures
Propulsion	2820	Fuel Crossfeed Valve failures
Propulsion	2810	Fuel Leaks
Propulsion	72	Engine Icing resulting in damage
Propulsion	2830	Inadvertent Fuel Jettison/Failure to jettison on command
Propulsion	7830	Loss of Thrust Reverser/Indications/Malfunctions
Propulsion	7170	Nacelle/Strut Drain blockage
Propulsion	2610	Overheat/Fire Detector failures
Propulsion	72	Uncontained Engine Failure
Propulsion	28	Unplanned Fuel Balance
Structure	51	Fuselage Panel Buckling to determine the no-tear-strip design
Structure	51	Loss of any aircraft panels; Subsequent damage to empennage

A.3 AIRCRAFT MANUFACTURERS CLASSIFICATION LIST BY SYSTEM'S CLASSIFICATION EXAMPLE

The objective of the following table is to describe a sample list of significant Failure Conditions from the perspective of an aircraft manufacturer. The failure condition severity has been classified based on service experiences of aircraft and/or traditional assumptions. Its sole purpose may be to assist users to derive the severity level of the event under consideration by first identifying the "Failure Condition" and its severity, which could be initiated by the event.

This table addresses general applicability, it is intended to be an example list and not an inclusive or prescriptive checklist, and it should not be utilized to replace any specific guideline intended for a particular aircraft type and configuration. It may not include all the information necessary for appropriate Failure Conditions of an aircraft with its various functions and its intended use. It should be emphasized again that this generic list of significant Failure Conditions example should not be applied indiscriminately to a particular aircraft type and configuration.

The classification of the consequences and the definitions below, have been paraphrased from advisory material:

1. **Catastrophic:** Failure Conditions which would result in multiple fatalities, usually with the loss of the aircraft, or would prevent continued safe flight and landing.

2. Hazardous: Failure Conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be:
 - a. A large reduction in safety margins or functional capabilities;
 - b. Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
 - c. Serious or fatal injury to a relatively small number of the occupants other than the flight crew.
3. Major: Failure Conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.
4. Minor: Failure Conditions which would not significantly reduce aircraft safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.
5. No Safety Effect: Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the aircraft or increase crew workload.

Table A2 - Aircraft manufacturers failure condition by system list example

Systems				
	Classification of Failure Condition			Comment
Function	Total Loss of Function with warning	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of attitude information to control roll and pitch	Catastrophic	Catastrophic, if includes both PFDs. Major, if includes one pilot's PDF.	Catastrophic	
Display of heading	Catastrophic Major if Navigation systems operational	Major	Catastrophic Major if Navigation systems operational.	
Display of altitude information	Hazardous	Minor	Catastrophic	
Display of airspeed information	Hazardous, during landing; otherwise, major	Minor	Hazardous	
Display of rate of turn	Minor	Minor	Minor	
Display of slip-skid	Minor		Minor	
Display of time	Minor		Major	
Display of navigation information	Major Total loss of navigation and communication is Catastrophic	Major	Major. Catastrophic for precision approaches.	
Communication	Major.	Minor	Major, if data link is primary.	
Visibility during landing	Hazardous			
Misinterpretation of flying altitude	Hazardous		Catastrophic	Occur during landing and poor visibility.
Display of radio altitude	Minor		Minor	Category I IFR.
Display of vertical speed	Major		Major	Category I IFR.
Display of flight guidance commands (Category I operation)	Minor		Minor	Category I ILS. For Category II ILS, an autopilot or flight director is required.
Autopilot failure	Minor, with warning. Major, without warning. Hazardous, if without warning during autoland.		Major, single axis and limited authority. Hazardous, multi-axis and limited authority. Catastrophic, if authority is unlimited.	Maximum inputs (hardovers) or (slowovers) to aircraft primary control surfaces should not exceed aircraft structural limits.

Systems				
	Classification of Failure Condition			Comment
Function	Total Loss of Function with warning	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Flight controls for pitch axis	Catastrophic	Major	Catastrophic	
Flight controls for roll axis	Hazardous, if yaw axis is still available	Major	Catastrophic	
Flight controls for yaw axis	Minor to Major, Hazardous to Catastrophic if combined with engine failure or severe cross wind	Minor	Catastrophic	
All hydraulics	Catastrophic			
Manual control flight controls	Catastrophic			
Artificial feel	Variable severity.			Variable severity needs to be evaluated on a case-by-case basis.
Takeoff director and automatic landing system	Catastrophic		Catastrophic, if malfunction of autoland below alert height. Hazardous, if takeoff director provides only lateral guidance.	
Stability augmentation	Variable severity	Minor	Variable severity	Variable severity needs to be evaluated on a case-by-case basis.
Stick pusher failure	Hazardous, if stall regime encountered. Otherwise, Minor.	Minor	Hazardous/ Catastrophic near ground	
Stick shakers/stall warning	Minor	Minor	Major	Assumes that a warning system is in place to notify pilot that loss of system function has occurred (for example, stick force changes, buffeting, inherent aerodynamics features, etc.).

Systems				
	Classification of Failure Condition			Comment
Function	Total Loss of Function with warning	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Trim control	Minor	Minor	Major, if manual trim. Catastrophic or Hazardous for electrical.	Major, for trim runaways if there is a trim-in-motion aural alert. Hazardous or Catastrophic, for trim runaways without a failure indication depending on trim authority.
Display of trim indications	Minor	Minor	Variable severity	Variable severity to be reviewed on a case-by-case basis.
Landing gear control	Hazardous	Minor	Major to Hazardous	
Display of landing gear indications	Major		Hazardous	
Brake control	Catastrophic, if unannounced loss of braking. Major, if annunciated loss of braking.	Hazardous	Hazardous	Electronic anti-skid and brake systems can cause significant ground handling problems if they malfunction under adverse conditions due to asymmetrical loading.
Visual warnings, cautions, and alerts	Major, for worst case			Failure Conditions depend on the criticality of systems being monitored and pilot action required.
Display of air temperature	Minor		Minor	
Overspeed warning	Minor	Minor	Minor	Airspeed may be used as a backup to the overspeed warning for continued safe flight and landing.

Systems				
	Classification of Failure Condition			Comment
Function	Total Loss of Function with warning	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Aural warnings				Failure Conditions depend on the criticality of the system.
Electrical system indication	Minor	Minor	Major	Depends on crew reference and analysis.
Vacuum/pressure indication	Minor	Minor	Major	Provides an indication that flight instruments are operating within power source limits.
Electrical power	Catastrophic, if primary flight instruments require electrical power	Hazardous for IFR. Depends upon capability of secondary power system.	Installation dependent	Depends on electrical system loads and the criticality of the functions.

Powerplant		
Failure Condition	Classification of Failure Conditions	Comment
Impact Damage to the Aircraft, Systems, or Occupants from Released Powerplant Components		
Released propeller blades	Catastrophic	Worst case assumption.
Uncontained disk or impeller failures	Catastrophic	Worst case assumption.
Engine/pylon separations	Catastrophic	Worst case assumption.
Engine case rupture	Catastrophic	Worst case assumption.
Uncontained blade failures	Hazardous	Uncontained fan blade failures, or uncontained turbine blade failures, or uncontained compressor blade failures.
Core cowl separations	Catastrophic	Worst case assumption.
Inlet cowl separations	Catastrophic	Worst case assumption.
Fan cowl separations	Hazardous	
Nozzle separations	Hazardous	
Liberation of large nacelle/fairing parts	Hazardous	
Liberation of small nacelle/fairing parts	Major	
Thermal Damage to the Airframe, Systems, or Occupants due to Excessive Heat Transfer from the Power Plant Installation		
Fire damage outside designated fire zones	Catastrophic	Caused by ignition of power plant flammable fluids initiated within fire zone (fire conditions exceed firewall criteria, or fire with pre-existing firewall failure) or outside fire zone (fire within flammable fluid carrying components, or fire in areas exposed to flammable fluid leakage).
Fire damage within designated fire zones	Hazardous	Caused by ignition of power plant flammable fluids.
Magnesium fires	Hazardous	
Electrical fires	Variable severity	Case-by-case review.
Loss of power plant installation thermal insulation	Variable severity	Case-by-case review.
Inadvertent release of engine (or APU) bleed air	Variable severity	Case-by-case review.
Inadvertent engine (or APU) exhaust gas impingement	Variable severity	Case-by-case review.
Distress of the Airframe, Systems, or Occupants due to Excessive Power plant Loads		
Excessive engine (or APU) vibration	Variable severity	Case-by-case review.
Explosive ignition of flammable vapors	Catastrophic	
Rupture of pressurized components	Hazardous	
Engine (or APU) seizure loads	Hazardous	

Powerplant		
Failure Condition	Classification of Failure Conditions	Comment
Abnormal thrust vectors	Variable severity	Caused by engine mount failures, or inadvertent thrust reverser deployment, or inadvertent application of propeller brake in flight, or inadvertent propeller beta pitch, or compressor surge or inlet separation /unstart, or nozzle failures, or compressor or inlet surge.
Failure to feather propeller when needed	Variable severity	Case-by-case review.
Uncommanded propeller feathering	Variable severity	Case-by-case review.
Separated powerplant components	Variable severity	Case-by-case review.
Fuel imbalance	Variable severity	Caused by asymmetric loading or use of fuel, or leaking or trapped fuel, or improper fuel transfer.
Loss of Thrust ¹ Required to Meet Certification or Operational Performance Requirements		
Thrust loss (detected) ~2 to ~55% (Twins) ~2 to ~38% (Tris) ~2 to ~30% (Quads)	Minor to Hazardous depend on scenario ²	Takeoff abort/over-run from takeoff power set to V1.
Thrust loss (detected) ~2 to ~55% (Twins) ~2 to ~38% (Tris) ~2 to ~30% (Quads)	Minor to Major depend on scenario ³	Air turn back/diversion any time after V1.
Thrust loss (undetected) ~2 to ~55% (Twins) ~2 to ~38% (Tris) ~2 to ~30% (Quads)	Minor to catastrophic depend on scenario ⁴	Unable to clear obstacle during any flight phase.
Thrust loss (detected) > ~55% (Twins) > ~38% (Tris) > ~30% (Quads)	Minor to Hazardous depend on scenario ²	Takeoff abort/over-run from takeoff power set to V1.
Thrust loss (undetected) > ~55% (Twins) > ~38% (Tris) > ~30% (Quads)	Catastrophic	Over-run/unable to clear obstacle from takeoff power set to V1.

¹ Percent is of total airplane thrust. Threshold values are based on typical margins. Thrust reductions caused strictly by pilot error are not considered a "Thrust Loss Scenario" for the purposes of this table.

The failure condition severities noted here are based solely on the effects of thrust loss and not on any other potential effects of causal failures (e.g., the potential hazards associated with damage from an uncontained engine failure, or loss of electrical or hydraulic systems are not reflected here). Therefore, these severities are generally depend on the effects the thrust loss scenario has on aircraft performance relative to certified field length or obstacle clearance limits (i.e., refer to 14 CFR Part 121 Subpart I and 14 CFR Part 25 Subpart B).

² The worst case scenario is where the thrust loss is such that it occurs throughout the takeoff roll but is only detected at or near V1 and the aircraft is too far down the runway to avoid a high speed over-run.

³ The severity of the effects from these performance losses will be dependent on the airplane type design, the mission, and the scenario.

⁴ The two scenarios here which produce the greatest risk of striking an obstacle, either during takeoff or enroute, are: a) operating for an extended period of time with a small symmetric thrust loss (2 to 15%) followed by an engine failure; and b) operating for a short period (perhaps a flight or two) with a larger thrust loss.

Powerplant		
Failure Condition	Classification of Failure Conditions	Comment
Thrust loss > ~55% (Twins) > ~38% (Tris) > ~30% (Quads)	Catastrophic	Unable to maintain altitude during takeoff between V1 and 1500 feet AGL.
Thrust loss > ~55% (Twins)	Catastrophic	Unable to maintain altitude during enroute.
Thrust loss (detected) ~38 to ~71% (Tris) ~30 to ~60% (Quads)	Minor to Major depend on scenario	An air turn back/diversion during enroute.
Thrust loss (undetected) ~38 to ~71% (Tris) ~30 to ~60% (Quads)	Minor to Catastrophic depend on scenario	Unable to clear obstacle during enroute.
Thrust loss > ~71% (Tris) > ~60% (Quads)	Catastrophic	Unable to maintain altitude during enroute.
Inadvertent inflight thrust reversal	Hazardous to Catastrophic	Between V1 and landing.
Loss of reverse thrust	Minor to Catastrophic	During landing or rejected takeoff. Severity dependent on runway condition
Loss of thrust control required to meet certification or operational controllability, maneuverability, or crew work load requirements	Major to Catastrophic	Caused by asymmetric thrust beyond that accommodated by flight control margins, or operation outside certified engine (or APU) limits, or unstable/unpredictable engine (or APU) operation which significantly impact crew workload.
Loss of system redundancy or functionality due to engine (or APU) failure	Variable severity	Caused by loss of electrical power generation, or hydraulics pumps, or ECS bleed air, or anti-ice bleed air. Case-by-case basis.

Distress of the Airframe, Systems, or Occupants due to Powerplant Display Failures				
	Classification of Failure Conditions			Comment
Function	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of fuel level indication	Minor	Minor	Major	
Display of powerplant indication tachometer	Minor	Minor	Minor	
Display of powerplant indication coolant temperature	Minor	Minor	Major	
Display of powerplant indication oil pressure	Minor	Minor	Minor	Assumes oil temperature is used as a backup.
Display of powerplant indication oil temperature	Minor	Minor	Minor	Assumes oil pressure is used as a backup.
Display of powerplant indication manifold pressure	Minor	Minor	Minor	Assumes backup use of Engine Gas Temperature (EGT), and fuel flow readings.
Display of powerplant indication fuel pressure	Minor	Minor	Major	
Display of powerplant indication gas temperature	Minor	Minor	Major	
Display of powerplant indication fuel flow	Minor	Minor	Major	
Display of powerplant fire warning	Major	Major	Hazardous	
Display of powerplant indication thrust	Major	Minor	Hazardous	
Display of powerplant thrust reverser position	Major		Major	
Display of powerplant torque	Minor	Minor	Major	
Display of power plant propeller blade angle	Major	?	Hazardous	

Ice Protection		
Function	Classification of Failure Conditions	Comment
Propeller, inlet, engine, or other powerplant ice protection on multiple powerplants when required	Hazardous	
Engine/powerplant ice detection	Hazardous	
Activation of engine inlet ice protection above limit temperatures	Hazardous	

Fuel System		
Function	Classification of Failure Conditions	Comment
Fuel feed/fuel supply	Catastrophic	
Fuel tank integrity	Catastrophic	
Fuel jettison	Hazardous	In case it is needed
Uncommanded fuel jettison	Hazardous to Catastrophic	

Cabin Decompression & Structural Failure		
Failure Condition	Classification of Failure Conditions	Comment
Control surfaces structural failures	Hazardous to Catastrophic	
Cabin decompression	Hazardous to Catastrophic	
Under-carriage structural failure on hard landing or soft ground	Catastrophic	
Loss of vent and pressurization (fuel system)	Catastrophic	Occurs during max/normal rate climb, or cruise, or max/ normal rate descent.

Fire Risk		
Failure Condition	Classification of Failure Conditions	Comment
Fire risk due to oxygen	Catastrophic	
Fire risk due to overheating brakes or wheel bays	Catastrophic	
Fire risk due to electric faults in equipment	Catastrophic	
Other Risks		
Wheels up landing	Hazardous	
Loss of ice protection when required	Hazardous	
Loss of cabin egress capability	Hazardous to Catastrophic	

A.4 AIRLINE CLASSIFICATION LIST EXAMPLE

This chapter provides examples of safety related events as considered by airlines for safety assessment process monitoring parameters. This is intended to be an example list and not a checklist since it may not include all the information necessary for a safety assessment process monitoring parameter list. Listed below are examples of safety assessment process monitoring events other than the reportable events required by 14 CFR Part and the categories are derived by a non-representative survey among several airlines.

An event can be placed in multiple categories based upon the individual specific effects.

Category 1 - Catastrophic/Near Catastrophic

The event/condition involves failure(s) that have or could result in a catastrophic accident.

Category 2 - Airworthiness/Safety Significant

A Category 2 event is an event, which has an adverse effect on safety. This may be as extensive as an adverse effect on level of safety intended in the certification process.

Category 2 events also include those events that must be reported to the Airworthiness Authorities in accordance with 14 CFR requirements or in accordance with a mutual agreement between the airframe manufacturer, supplier, or operators and Airworthiness Authorities. In addition, Category 2 events may also include those that are specified by the Airworthiness Authorities.

In addition, Category 2 events may be events, which have an adverse effect on the company internal level of safety.

The following guidelines can be used to assist in determining if the event is a Category 2 event:

1. This event/condition (or similar past occurrence) contributed to an aircraft accident or serious incident.
2. An event/condition which brings the aircraft within one probable failure of an accident.
3. The event (personal safety issue independent of aircraft level concerns) could be expected or has resulted in serious injury to flight/cabin crew, passengers, maintenance, or service personnel.
4. An event/condition that is considered to be a safety issue, provided justification and rationale is presented.

Examples of Category 2 events include:

- a. Significant autopilot anomalies (pitch up, hardovers, etc.)
- b. Over-rotation (takeoff and landing tail strike)
- c. High energy rejected takeoff
- d. Runway excursions during takeoff or landing (excluding taxi)
- e. Sustained loss of cabin pressure control
- f. Severe turbulence causing aircraft damage and/or personnel injury

Category 3 - Impact on perceived safety

A Category 3 event is an event, which has no real impact on aircraft safety but is perceived as a safety item.

Examples of Category 3 events are as follows:

- a. Smoke in cabin
- b. Oxygen mask deployment
- c. Airframe/engine vibration
- d. Toilet system shut down
- e. Temporary loss of thrust or power, or any other malfunction of the propulsion system, which does not impair aircraft controllability or structural integrity
- f. Air turn back or diversion

Category 4 - Impact on operation, reliability or passenger comfort

A Category 4 event is an event that:

1. Degrades the aircraft operational reliability, affects scheduled or line maintenance, generates reliability issue or,
2. Makes passengers feel physically uncomfortable and that would likely result in complaints from the passengers.

Examples of Category 4 events are as follows:

- a. Late departure
- b. Return to gate due to failures
- c. Cabin temperature too high/low
- d. Cabin too noisy

Table A3 - Airline Classification List Example

Ref.	Structural events	Category
3.1.1.	Damage or structural failures that adversely affect the structural strength, performance or flight characteristics of the aircraft, and that would normally require major repair or replacement of the affected components.	2
3.1.2.	Nicks, dents and small penetrations in aircraft primary structure.	3
3.1.3.	Hard Landings (>12 ft/s).	2
3.1.4.	Physical loss of control surfaces including control tabs.	1
3.1.5.	Cracks in fuselage pressure bulkheads.	2
3.1.6.	Cracks in primary structure.	2
3.1.7.	Landing gear vibration or shimmy.	2
3.1.8.	Control surface vibration/flutter.	2
3.1.9.	Excessive engine vibration (>3-4 points).	2
3.1.10.	Foreign Object Damage (FOD) to nacelles, pylons, or primary structure.	2
3.1.11.	Stiff or frozen control surfaces.	1
3.1.12.	Cabin window problems (excluding crazing).	2
3.1.13.	Cockpit window problems (excluding crazing).	2
3.1.14.	Windshield problems (excluding electrical).	3
3.1.15.	Bird strikes.	3
3.1.16.	Severe turbulence encounters.	2
3.1.17.	CG load factor excursions exceeding ± 1 g.	2
3.1.18.	Ground handling problems such as jacking failures or tow bar failures.	4
3.1.19.	Tail strikes.	2
3.1.20.	Fuel leaks in structural wing tanks.	2
3.1.21.	Overweight landings.	3
3.1.22.	Loss of nacelles.	2
3.1.23.	Incidents of control surface unbalance.	2
3.1.24.	Control surface buzz	2
3.1.25.	Failure of interior item attach members such as overhead storage bins, galleys, or lavatories.	4
3.1.26.	Failures of cabin negative pressure relief valves.	2
3.1.27.	Structural corrosion in areas not covered by corrosion ADs or ALIs.	2
3.1.28.	Structural failures in seats and/or their attach structure.	2
3.1.29.	Incidents of structural overheating.	2
3.1.30.	Parts becoming detached from the aircraft in-flight.	2
Ref.	Electrical Systems	Category
3.2.1.	Complete loss of electrical power.	1
3.2.2.	Complete loss of normal electrical power.	2
3.2.3.	Electrical system failure in which more than 50% of the aircraft's normal generating capacity is lost.	2
3.2.4.	Electrical system failure of malfunction in which more than 50% of the required electrical power was affected including transients, out of tolerance voltage or frequency, and wire bundle/feeder damage.	2
3.2.5.	Chafing/Arising/Sparking of power feeders and/or wires or wire bundles.	2
Ref.	Hydraulic Systems	Category
3.3.1.	Multiple hydraulic system failures, this includes any occurrence in which more than 50% of the main hydraulic systems fail.	2
Ref.	Propulsion	Category
3.4.1.	Any uncontained release of debris from a rotating component malfunction.	1
3.4.2.	Case ruptures.	2
3.4.3.	Case burn through.	2
3.4.4.	Under cowl fires and APU fires.	1
3.4.5.	High pressure air leak due to casing or high pressure air duct system malfunction.	2
3.4.6.	Engine separation.	1
3.4.7.	Cowl separation.	2

3.4.8.	Thrust reverser malfunction including uncommanded deploy/stow and failure to deploy/stow when commanded inappropriate operation.	2
3.4.9.	Loss of ability to control or shutdown engine.	2
3.4.10.	Loss of critical engine indicating systems on more than one engine.	2
3.4.11.	Uncommanded fuel transfers.	2
3.4.12.	Uncommanded automatic thrust changes or autothrottle movement.	2
3.4.13.	Engine imbalances.	3
3.4.14.	Failure of all fuel pumps in a single fuel tank.	2
3.4.15.	Fuel pump arcing.	1
3.4.16.	Total loss of fuel quantity indication, a failure, or malfunction of a fuel quantity indicator that results in erroneous fuel quantity indication.	2
3.4.17.	Engine shutdown/flameout which is caused by fuel starvation.	2
3.4.18.	Engine shutdown which is caused by airframe ice ingestion, bird ingestion, or ingestion of an airframe part.	2
3.4.19.	In-flight engine restart after a flameout (both successful and failed attempts).	2
3.4.20.	Engine flameout events.	2
3.4.21.	Multiple engines inoperative, including any occurrences in which more than 50% of the engine thrust is affected.	1
3.4.22.	A deficiency that leads to a total loss of power or thrust due to common mode failure.	1
3.4.23.	Failures, malfunction, or defect of any aircraft component of system that causes an uncommanded thrust change at altitudes below 3000 feet.	2
3.4.24.	Failures, malfunction, or defect of an engine overspeed protection.	2
3.4.25.	Failures, malfunction, or defect of a fuel shutoff system component that affects fuel flow or causes hazardous leakage during flight.	2
Ref.	Flight Controls	Category
3.5.1.	Uncommanded deflection of any elevator, aileron, or rudder.	2
3.5.2.	Failure of any elevator, aileron, or rudder to deflect when commanded.	2
3.5.3.	Failure of any or all flap sections to extend or retract.	2
3.5.4.	Uncommanded extension or retraction of any or all flap sections.	2
3.5.5.	Failure of any or all slat sections to extend or retract.	2
3.5.6.	Uncommanded extension or retraction of any or all slat sections.	2
3.5.7.	Failure of any or all spoiler sections to extend or retract.	2
3.5.8.	Uncommanded extension or retraction of any or all spoiler sections.	2
3.5.9.	Jamming of any primary or secondary flight control surface.	2
3.5.10.	Actuator shaft runaways.	2
3.5.11.	Actuator shaft jams.	2
3.5.12.	Actuator shaft releases.	2
3.5.13.	Broken actuator shafts and/or casings.	2
3.5.14.	Loss or malfunction of any load feel spring or load feel system.	2
3.5.15.	Any reversion of a fly-by-wire flight control system from a normal mode to alternate mode or backup mode.	2
Ref.	Systems related event	Category
3.6.1.	Single system failure if aircraft damage results or flying (handling) qualities affected.	2
3.6.2.	Multiple failures in redundant subsystems occurring after dispatch.	2
3.6.3.	Common failures that affect multiple systems, including human-caused errors such as those from flight or maintenance crews.	2
3.6.4.	Failures involving the rapid release of stored energy including oxygen, firex, accumulators, cables, etc.	2
3.6.5.	Disintegrating tires or wheel (gear up or gear down).	2
3.6.6.	Rotating machinery failure/non-containment including any rotating machinery (engines, auxiliary power unit, air cycle machine, or ram air turbine) failure that penetrates the case regardless of damage.	2
3.6.7.	Hot air duct ruptures or leaks.	2
3.6.8.	Failure of Oxygen masks to deploy.	2
3.6.9.	Inadvertent oxygen mask deployment.	4
3.6.10.	A deficiency that affects back up emergency systems.	3

Ref.	Air Data	Category
3.7.1.	Loss of all altitude data for all displays including standby.	1
3.7.2.	Loss of primary altitude data on both pilots and copilots displays.	2
3.7.3.	Abnormal altitude data on both pilots and copilots displays.	2
3.7.4.	Abnormal altitude data on one pilots display compounded by inappropriate crew action.	2
3.7.5.	Loss of all airspeed data for all displays including standby.	1
3.7.6.	Loss of primary airspeed data on both pilots and copilots displays.	2
3.7.7.	Abnormal airspeed data on both pilots and copilots displays.	2
3.7.8.	Abnormal airspeed data on one pilots display compounded by inappropriate crew action.	2
3.7.9.	Loss of vertical speed data on both pilots and copilots displays.	2
Ref.	Attitude/Heading	Category
3.8.1.	Loss of all attitude information for all displays including standby.	1
3.8.2.	Loss of primary attitude information on both pilots and copilots displays.	2
3.8.3.	Abnormal roll or pitch attitude on both pilots and copilots displays.	2
3.8.4.	Abnormal roll or pitch attitude data on any one display.	2
3.8.5.	Loss of all heading data for all displays including standby.	2
3.8.6.	Loss of heading data on both pilots and copilots displays.	2
3.8.7.	Abnormal heading data on both pilots and copilots displays.	2
3.8.8.	Abnormal heading data on one pilots display compounded by inappropriate crew action.	3
Ref.	Warning Systems	Category
3.9.1.	Loss of aural warnings.	3
3.9.2.	Nuisance aural warnings.	3
3.9.3.	Nuisance TCAS resolution advisories.	3
3.9.4.	Failure to provide TCAS traffic advisories or resolutions.	2
3.9.5.	Nuisance wind shear alerts.	3
3.9.6.	Failure to alert wind shear conditions during takeoff and approach.	2
3.9.7.	Ground Proximity Warning System (GPWS) alert, exclude false alert.	2
3.9.8.	False annunciation of "Warnings" and "Cautions" during takeoff and approach.	2
Ref.	Navigation Systems	Category
3.10.1.	Loss of any or all navigation information on both pilots displays.	2
3.10.2.	Display of abnormal navigational or positional information on both pilots displays.	2
3.10.3.	Display of abnormal navigational or positional information on an one display compounded by inappropriate crew action.	2
3.10.4.	Loss of ILS information on both pilots displays.	3
3.10.5.	Abnormal ILS information on both pilots displays.	2
3.10.6.	Abnormal ILS information on any one display compounded by inappropriate crew action.	2
3.10.7.	Loss of radio altimeter data on both pilots displays.	3
3.10.8.	Loss of radio altimeter data on any one display during approach and landing.	3
3.10.9.	Abnormal radio altimeter data on both pilots displays.	2
3.10.10.	Abnormal radio altimeter data on any one display during approach and landing.	3
3.10.11.	Loss of more than 50% of the flight guidance or navigation systems.	2
3.10.12.	Runway excursions during takeoff or landing.	1
Ref.	Stall Warning Systems	Category
3.11.1.	Activation of stall warning or stick shaker when aircraft is not in stall regime.	2
3.11.2.	Failure of stall warning or stick shaker when aircraft is in stall regime.	2
3.11.3.	Failure to command stick pusher when aircraft is in stall regime.	2
3.11.4.	Activation of stick pusher when aircraft is not in stall regime.	2

Ref.	Communications	Category
3.12.1.	Loss of all communication.	2
3.12.2.	Loss of all VHF communications.	3
3.12.3.	Loss of all HF communications.	3
3.12.4.	Radio Transceiver stuck in transmit mode.	3
Ref.	Automatic Flight Control Systems	Category
3.13.1.	Erroneous guidance of Flight Director and/or Autopilot.	3
3.13.2.	Autopilot hardovers.	2
3.13.3.	Oscillatory autopilot failures.	3
3.13.4.	Erroneous autopilot pitch trim.	3
3.13.5.	Loss of autopilot disconnect function.	3
3.13.6.	Erroneous autopilot engagement.	3
3.13.7.	Uncommanded autopilot disconnects without disconnect alerts.	3
3.13.8.	Other significant autopilot anomalies.	3
3.13.9.	Uncommanded autopilot disconnects during fail-operational auto lands.	2
3.13.10.	Autopilot slowovers.	3
3.13.11.	Flight deck automation system or component failure and/or anomaly that adversely affects safe flight path management.	2
Ref.	External Environmental Events	Category
3.14.1.	Lightning strikes or static discharge events that result in structural, electrical (direct or indirect effects) or fuel related effects.	3
3.14.2.	Events which are thought to be a result of High Intensity Radiating Fields (HIRF) or Electro-Magnetic Interference (EMI).	2
3.14.3.	Ice formation and shedding events including ice in the air data system, freezing of mechanical flight controls, or inability to start up or improper operation as result of cold soak.	2
3.14.4.	Wind shear near the ground.	2
3.14.5.	Foreign object strike including birds, hail, or runway debris that affects any aircraft structure of system.	3
3.14.6.	Midair collisions.	1
Ref.	Aircraft Motion or Flight Path Events	Category
3.15.1.	Over rotation events including takeoffs, landings, and tail strikes.	2
3.15.2.	Severe turbulence or aerodynamic upset including any momentary loss of aerodynamic stability or control, hardovers or partial hardovers at any rate, evasive action to avoid a midair collision, low-speed or high-speed stall, and high-speed/high-g buffet.	2
3.15.3.	Rapid decompression or rapid descent.	2
3.15.4.	Loss of control during takeoff, landing, or taxi including overruns, icy or wet runways, and hydroplaning and/or any braking related problems.	1
3.15.5.	Approach errors including not landing on the runway or partially landing on the runway, and hard landings.	1
3.15.6.	Belly landings including failure of any landing gear component, landing with any gear retracted.	1
3.15.7.	Ditching events.	1
3.15.8.	Aircraft structures, components, or materials departing aircraft.	2
3.15.9.	Uncommanded or inadvertent opening of passenger doors, cargo doors, or emergency exits during any phase of flight.	1
3.15.10.	Rejected Takeoffs (RTOs) that exceed 100 knots.	2
3.15.11.	Severe turbulence causing aircraft damage and/or personnel injury.	2
3.15.12.	Dangerous positioning on final.	2
Ref.	Crew Problem In-Flight	Category
3.16.1.	Affecting the crew's ability to perform intended functions.	2
3.16.2.	Flight crew errors such as judgment, inattention, habit pattern, navigation, response to ATC, inadvertent system operation, and any combination of inadequate procedure, crew error.	2

Ref.	Ground Events	Category
3.17.1.	Any aircraft evacuation.	2
3.17.2.	Collision on the ground.	1
3.17.3.	Ground crew injury.	1
3.17.4.	Inadvertent operation of evacuation slides.	3
3.17.5.	Failures of an evacuation slide to deploy properly.	2
3.17.6.	Inability to open or close passenger doors, cargo doors, or emergency exits.	3
3.17.7.	Off taxiway excursion resulting in aircraft damage.	2
3.17.8.	Damage to the tug, tow bar, or aircraft components during pushback.	3
3.17.9.	Dragging any structure on the ground.	3
Ref.	Fires	Category
3.18.1.	Any fire on the aircraft in the air or on the ground.	1
3.18.2.	Any smoke, odor, or fumes in the cockpit or cabin.	2
3.18.3.	Any heat or fire related damage including charred material, soot deposits, or heat related discoloration.	2
3.18.4.	Loss or degradation of fire detection/protection or extinguishing capability.	2
Ref.	Other	Category
3.19.1.	Any occurrence that has serious potential for resulting in an incident.	2
3.19.2.	Gross cargo shift, weight or center of gravity errors.	2
3.19.3.	Personnel injury.	2
3.19.4.	A deficiency that affects systems used to locate the site of a crash (Emergency Locator Transmitter).	2
3.19.5.	A deficiency that affects Cockpit Voice Recorder, Flight Data Recorder systems.	3

A.5 CROSS-REFERENCE LIST

The objective of the following table is to provide the cross-reference between the sample list of significant Failure Conditions as shown in Section A.2 of this appendix and the list of airline significant events from Section A.3. This should allow the airlines to judge how safety significant the failure condition could become compared to the original assumptions of the aircraft manufacturer. This table addresses general applicability, and it should not be utilized to replace any specific guideline intended for a particular aircraft type and configuration.

This is intended to be an example list and not an inclusive or prescriptive checklist since it may not include all the information necessary for appropriate failure conditions of a transport aircraft with its various functions and its intended use.

Table A4 - Significant failure conditions list to airline significant events cross reference

Propulsion Systems										
Classification of Failure Conditions										
Function		Total loss of function (detected)			Loss of primary means of providing function/partial loss of function			Uncommanded/Misleading/malfunction non detected or not clarified		
Ref	Category or Type	Failure Condition	Classification/ comments	AL Ref	Failure Condition	Classification/ comments	AL Ref	Failure Condition	Classification/ comments	AL Ref
1	Containment	Uncontained release of major debris (Disc/disc rim)	Major / Cat. Dependent on the aircraft effect	3.4.1 3.4.2	Uncontained release of minor debris (Blades)	Minor/Major Dependent on the aircraft effect	3.4.1 3.4.2	NA		
2	Fire containment	Engine fire a. Undetected b. Detected / uncontrolled	a. Potentially Cat. b. Potentially Cat.	3.4.3 3.4.4	Failure of one loop of a dual loop fire detection system Failure of one shot of fire extinguishing system	Minor	3.4.3 3.4.4	False fire warning (engine shut down) False warning of fire bottle discharge	Minor Minor	3.4.10 ?
3	Engine retainment	Engine separation	Major / Cat.	3.4.6	Engine retainment partial failure	Minor / Major	3.4.6	NA		
4	Thrust reverse	Failure to deploy	Minor to Catastrophic dependent on runway condition	3.4.8	NA			Erroneous indication	Minor	3.4.8
5	Thrust reverse	Failure to stow	Minor / Major	3.4.8	NA			Erroneous indication		
6	Thrust reverse	Inadvertent deployment	Major / Cat.	3.4.8	Inadvertent partial deployment	Major / Cat.	3.4.8	Non detected deployment	t.	3.4.8
7	Thrust reverse	Inadvertent stowage	Minor / Major	3.4.8	Inadvertent partial stowage	Minor / Major	3.4.8	Non detected stowage		8
8	Engine control	Loss of control (FADEC)	Minor	3.4.9	Partial loss of control (One lane)	Minor	3.4.9	Unwanted thrust change	Minor / Cat	3.4.9
9	Engine control	Inability to shut down	Major / Cat.	3.4.9	a. Complete loss of throttle control b. Loss of engine shut down handle capability	Major Major	3.4.9	Unwanted shut down	Major / Haz.	3.4.9
10	Indication	Complete loss of indication	Minor / Major	3.4.10	Partial loss of indication	Minor	3.4.10	Erroneous indication	Major / Cat	3.4.10

Flight Control										
		Classification of Failure Conditions								
Function		Total loss of function (detected)			Loss of primary means of providing function/partial loss of function			Uncommanded/Misleading/malfunction non detected or not clarified		
Ref	Cat or Type	Failure Condition	Classification/ comments	AL Ref	Failure Condition	Classification/ comments	AL Ref	Failure Condition	Classification/ comments	AL Ref
1	Lateral control (roll and yaw)	Loss of lateral control (roll and yaw)	CAT	3.5.2						
2	Roll control	Loss of roll control (Rudder being available)	HAZ	3.5.2	Partial loss of roll control	MIN to MAJ (depending on remaining roll rate)	3.5.2	Ailerons or roll spoilers runaway	MAJ to CAT depend on the number of surfaces affected (depends on flight phases)	3.5.1
3	Yaw control	Loss of yaw control (rudder) (Roll being available)	MIN - MAJ HAZ - CAT combined with engine failure. MAJ/HAZ combined with crosswind	3.5.2	Partial loss of yaw control	MIN MAJ to HAZ if combined with engine failure MIN to MAJ if combined with crosswind	3.5.2	Rudder runaway	CAT if unlimited runaway MIN to HAZ if oscillations	3.5.1
4	Pitch control (elevators and THS)	Total loss of pitch axis control (elevator and THS)	CAT	3.5.2	Loss of elevators or THS	MAJ to HAZ	3.5.2	Elevators or THS runaway	MAJ if transient runaway HAZ/CAT if unlimited runaway	3.5.1
5	Flaps / Slats	Loss of flaps and slats (Landing in clean condition)	MAJ	3.5.3 3.5.5	Loss of flaps or slats	MIN	3.5.3 3.5.5	Loss of flaps or slats without warning	CAT	3.5.3 3.5.5
								Flap		3.5.6
6	Ground spoilers	Total loss of ground spoilers		3.5.7	Partial loss of ground spoilers		3.5.7	Uncommanded extension of spoilers	CAT Depend on the flight phase	3.5.8

[illegible]

[illegible]

APPENDIX B - QUALITATIVE RISK ASSESSMENT

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

B.1 SCOPE

This appendix describes qualitative risk assessment, a procedure that allows a non-numeric evaluation of a flight safety issue. This analysis approach is often used by organizations when they are dealing with low level safety risks. This qualitative risk assessment also allows an organization to respond immediately with mitigating or corrective action on those issues identified with high perceived safety risk.

B.2 INTRODUCTION

This appendix describes how qualitative risk assessment can be a powerful tool within an organization's safety process. It provides a structured way to evaluate safety issues non-numerically. It is particularly useful when numerical data is missing or incomplete, making quantification of a safety risk difficult or impossible.

The qualitative analysis results are compared with the organization's formal risk criteria. Two example methods of accomplishing this comparison, Operator Hazard Level or a Hazard Risk Matrix, are presented.

B.3 CATEGORIZING SEVERITY

Many different schemes for classification of safety events are used successfully within the aviation industry. The success of a particular classification method depends not so much on its specific details, as much as it depends on it being a formal and consistent part of an organization's safety process.

Several classification schemes in common use within the aviation industry, are presented in this section. It should be noted that classifications of severity are different for different organizations. For example, an operator may classify an event as safety significant and a manufacturer may classify the same event as minor. Examples of these classification differences can be seen in Appendix A.

Note that the severity classifications shown are not limited to Qualitative Risk Analyses. Many were developed for use in Quantitative Risk Analysis (Appendix C) processes developed by industry and regulators. It is the methodology used to assess the probabilities of event occurrences at the various severity levels that primarily determines whether a risk analysis is qualitative or quantitative.

B.3.1 MIL-STD-882E

MIL-STD-882E, which defines the system safety process for development of United States military systems, defines four "hazard severity categories." The MIL-STD-882E categories are summarized in Table B1.

Table B1 - Hazard severity categories

<u>Description</u>	<u>Category</u>	<u>Definition</u>
CATASTROPHIC	I	Death, system loss, or severe environmental damage.
CRITICAL	II	Severe injury, severe occupational illness, major system, or environmental damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system, or environmental damage.
NEGLIGIBLE	IV	Less than minor injury, minor occupational illness, or minor system, or environmental damage.

The category definitions in MIL-STD-882E are intentionally broad enough to be applicable to a wide variety of programs, both in the aerospace and non-aerospace industries. In practice, these broad definitions typically provide a framework to help the military customer and military contractor develop more useful detailed definitions to be used on a specific program.

B.3.2 FAA Advisory Circular 25.1309-1A

FAA Advisory Circular(AC) 25.1309-1A provides guidance to assist airplane manufacturers in showing compliance with certification requirements stated in 14 CFR Part 25.1309. The Advisory Circular defines four categories of "failure conditions." The 14 CFR Part 25.1309 categories are summarized in Table B2.

Table B2 - AC 25-1309A failure conditions

<u>Description</u>	<u>Definition</u>
CATASTROPHIC	Failure conditions, which would prevent continued safe flight and landing.
MAJOR (MORE SEVERE CASES)	Failure conditions which would result in a large reduction in safety margins or functional capabilities, higher workload or physical distress such that the crew could not be relied upon to perform its tasks accurately or completely, or adverse effects on occupants.
MAJOR	Failure conditions which would result in a significant reduction of safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or some discomfort to occupants.
MINOR	Failure conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some inconvenience to occupants.

B.3.3 EASA Advisory Material Committee (AMC) 25.1309

EASA Acceptable Means of Compliance (AMC) 25.1309, which provides EASA guidance for safety requirements for the design of airplane systems, defines four categories of "Failure Conditions." The definitions of the four categories are very similar to the FAA AC25.1309-1A definitions in the previous section. The AMC categories are summarized in Table B3.

Table B3 - AMC 25.1309 failure categories

<u>Description</u>	<u>Definition</u>
CATASTROPHIC	Failure Conditions which would result in multiple fatalities, usually with the loss of the aircraft.
HAZARDOUS	Failure Conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: (i) A large reduction in safety margins or functional capabilities; (ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or (iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.
MAJOR	Failure Conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.
MINOR	Failure Conditions which would not significantly reduce aircraft safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.

B.3.4 CAAM Hazard Levels

A committee formed by the Aerospace Industries Association (AIA) developed another event categorization scheme, with applicability specifically for transport category airplane engines. The task of this committee was to define a Continued Airworthiness Assessment Methodologies (CAAM) which could provide the means to effectively prioritize safety related engine problems observed in service. As part of this prioritization process, events are categorized as presented in Table B4.

B.3.5 Engine Manufacturer (Example)

Table B5 provides an example of an event classification system used by an engine manufacturer.

B.3.6 Operator (Example)

Table B6 illustrates an event classification system used by an airline. Only propulsion systems events are shown, but Appendix A includes the complete list for all airplane systems.

Table B4 - CAAM hazard levels**Level 5 Catastrophic Consequences**

Catastrophic outcome - an occurrence resulting in multiple fatalities, usually with the loss of the airplane.

Level 4 Severe Consequences

- 4a. Forced Landing.
- 4b. Actual loss (Hull Loss) of aircraft (as opposed to economic) while occupants were on board.
- 4c. Serious Injuries or Fatalities.

Level 3 Serious Consequences

- 3a. Substantial damage to the airplane or second unrelated system.
- 3b. Uncontained (Uncontrolled) fires.
- 3c. Rapid depressurization of the cabin.
- 3d. Permanent loss of thrust greater than one propulsion system (inflight).
- 3e. Temporary or permanent inability to climb and fly 1000 feet above terrain.
- 3f. Temporary or permanent impairment of aircraft.
- 3g. Malfunctions or failures that result in smoke or other fumes, delivered through the ECS system, that result in a serious impairment.

Level 2 Significant Consequences

- 2a. Nicks, dents and small penetrations in airplane structure.
- 2b. Slow depressurization.
- 2c. Controlled fires (i.e., extinguished by on-board airplane systems).
- 2d. Fuel leaks beyond normal extinguishing capabilities, i.e., if fire had resulted.
- 2e. Minor injuries.
- 2f. Multiple propulsion system/APU malfunctions, or related events, where one engine remains shutdown but continued safe flight at an altitude 1000 feet above terrain along the intended route is possible.
- 2g. Any high speed takeoff abort.
- 2h. Separation of propulsion system, inlet, reverser blocker door, translating sleeve inflight without Level 3 damage consequences to the airplane structure or systems.
- 2i. Partial inflight reverser deployment or propeller pitch change malfunction(s) which do not result in loss of airplane control or damage to airplane primary structure.

Level 1 Minor Consequences

- 1a. Uncontained nacelle damage confined to affected nacelle/APU area.
- 1b. Uncommanded power increase, or decrease, at an airspeed above V1 and occurring at an altitude below 3000 feet.
- 1c. Multiple propulsion system malfunctions or related events, temporary in nature, where normal functioning is restored on all propulsion systems and the propulsion systems function normally for the rest of the flight.
- 1d. Separation of propeller/component releases which cause no other damage.
- 1e. Uncommanded propeller feather.
- 1f. Propulsion system (engine or propeller) malfunctions resulting in a load and frequency spectrum which exceeds the level demonstrated for compliance with 14CFR Parts 33.23, 25.361 or 25.903c or their equivalent (e.g., engine malfunctions resulting in an imbalance exceeding the level of imbalance demonstrated under 14CFR Part 33.94 or its equivalent).

Table B5 - Engine manufacturer classification system example

<u>Failure Category</u>	<u>Description/Examples</u>
I	14 CFR Part 33.75/CS-E Listed Hazards a) uncontained high energy engine debris b) loss of engine/gearbox/propeller structural support c) uncontrolled fire external to the engine d) loss of shutdown capability e) toxic fumes from engine bleed air entering the cabin f) thrust in the opposite direction to that demanded by the pilot g) other failure conditions judged to be of equivalent severity to a) through f)
II	Safety Devices a) safety device or system activated to preclude Category I failure condition (i.e., one failure away from a Category I event, e.g., overspeed protection utilized) b) safety device or system fails or becomes disabled (i.e., one failure away from a Category I event) c) other failure conditions judged to be of equivalent severity to a) or b); generally any failure condition that is one failure away from a Category I event
III	Loss of Thrust Control a) uncommanded total power loss b) uncommanded partial power loss, increase, or oscillation of a magnitude considered excessive for the application c) pilot-commanded power loss when action is a proper or reasonable response to an engine failure condition d) significant lack of response to a pilot's throttle lever movement e) uncommanded propeller pitch change resulting from an engine or engine control system malfunction f) other failure conditions judged to be of equivalent severity to a) through e)
IV	Minor all failure modes not listed as Category I, II, or III and for which the consequences are less serious than for Category III events

Table B6 - Operator classification example

<u>Failure Category</u>	<u>Description/Examples</u>
1.	Catastrophic a) any uncontained release of debris from a rotating component malfunction b) case rupture c) case burnthrough d) under cowl fires and APU fires e) engine separation f) multiple engine inoperative, including any occurrences in which more than 50% of the engine thrust is affected g) a deficiency that leads to a total loss of power or thrust due to a common mode failure
2.	Safety Significant a) high pressure air leak due to casing or high pressure air duct system malfunction b) cowl separation c) thrust reverser malfunction, including uncommanded deploy/stow and failure to deploy/stow when commanded d) loss of ability to control or shutdown engine e) loss of critical engine indicating systems on more than one engine f) uncommanded fuel transfers g) uncommanded automatic thrust changes or autothrottle movement h) failure of all fuel pumps in a single fuel tank i) fuel pump arcing j) engine shutdown/flameout which is caused by fuel starvation k) engine shutdown which is caused by airframe ice ingestion, bird ingestion, or ingestion of an airframe part l) inflight engine restart after a flameout event (both successful and failed attempts) m) engine flameout event n) failure, malfunction, or defect of any airplane component or system that causes an uncommanded thrust change at altitudes below 3000 feet o) failure, malfunction, or defect affecting engine overspeed protection p) a failure, malfunction, or defect of a fuel shutoff system component that affects fuel flow or causes hazardous leakage during flight
3.	Impact on Perceived Safety a) engine imbalances b) total loss of fuel quantity indication; failure, malfunction, or defect leading to an erroneous fuel quantity indication
4.	Impact on Operation, Reliability, or Passenger Comfort a) flight cancellation or delay for unscheduled engine maintenance

B.4 ASSIGNING PROBABILITY

The second major aspect of a qualitative risk assessment is assigning a probability category. The probability category is assigned based on judgment or similarity/historical data and is optimum when all available information is reviewed by all affected disciplines. Many different schemes for assigning probability categories are used successfully within the aviation industry. This section provides descriptions of several schemes in common use.

B.4.1 MIL-STD-882E

MIL-STD-882 E, which defines the system safety process for development of United States military systems, defines five "hazard probability levels." Table B7 presents the MIL-STD-882 E levels.

Table B7 - MIL-STD-882 e hazard probability levels

<u>Description</u>	<u>Level</u>	<u>(per) Specific Individual Item</u>	<u>(per) Fleet or Inventory</u>
FREQUENT	A	Likely to occur frequently	Continuously experienced
PROBABLE	B	Will occur several times in the life of an item	Will occur frequently
OCCASIONAL	C	Likely to occur sometime in the life of an item	Will occur several times
REMOTE	D	Unlikely but possible to occur in the life of an item	Unlikely but can be reasonably expected to occur
IMPROBABLE	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

B.4.2 FAA Advisory Circular 25.1309-1A

FAA AC 25.1309-1A provides guidance to assist airplane manufacturers in showing compliance with certification requirements stated in 14 CFR Part 25.1309. The Advisory Circular defines three "qualitative probability terms." These 14 CFR Part 25.1309 terms are summarized in Table B8.

Table B8 - AC 25.1309-1A probability terms

<u>Term</u>	<u>Description</u>
Probable	Anticipated to occur one or more times during the entire operational life of each airplane.
Improbable	Not anticipated to occur during the entire operational life of a single random airplane. However, it may occur occasionally during the entire operational life of all airplanes of one type.
Extremely Improbable	Not anticipated to occur during the entire operational life of all airplanes of one type.

B.4.3 EASA Acceptable Means of Compliance (AMC) 25.1309

EASA Acceptable Means of Compliance (AMC) 25.1309, which provides EASA guidance for safety requirements for the design of airplane systems, defines four "qualitative probability terms." These definitions are very similar to the FAA AC 25.1309-1A definitions in the previous section. The major difference is that the FAA term "Improbable" is divided into two terms, "Remote" and "Extremely Remote." Table B9 summarizes the AMC probability terms.

Table B9 - AMC 25.1309 probability terms

<u>Term</u>	<u>Description</u>
Probable	Anticipated to occur one or more times during the entire operational life of each aircraft.
Remote	Unlikely to occur to each aircraft during its total life but which may occur several times when considering the total operational life of a number of aircraft of the type.
Extremely Remote	Not anticipated to occur to each aircraft during its total life but which may occur a few times when considering the total operational life of all aircraft of the type.
Extremely Improbable	Not anticipated to occur during the entire operational life of all aircraft of one type.

B.4.4 Engine Manufacturer (Example)

Typically, an organization will establish probability categories and definitions that best fit its particular needs. As an example, Table B10 provides the terms used by one engine manufacturer. The terms are very similar to those used in MIL-STD-882E, but were edited somewhat for ease of use by this specific company.

Table B10 - Engine manufacturer probability categories example

<u>Term</u>	<u>Definition</u>
FREQUENT	Continuously experienced
PROBABLE	Occurs frequently
OCCASIONAL	Occurs several times
REMOTE	Unlikely to occur
IMPROBABLE	Extremely unlikely to occur

B.4.5 Operator (Example)

Table B11 lists the qualitative probability terms used by an airline. The airline established their own definitions, in order to tailor them to their own safety process.

Table B11 - Operator probability categories example

<u>Term</u>	<u>Definition</u>
EXTREME	Frequent occurrences (certain to happen often)
HIGH	Occasional occurrences (certain to happen at least once)
MODERATE	Likely to happen under normal operating conditions
LOW	Possible to happen under normal operating conditions
RARE	Possible, but only under specific conditions other than normal operations

B.5 RESOLUTION OF ASSESSMENT RESULTS

B.5.1 Operator Hazard Level

To assure efficient use of resources, the operator may choose to establish an “Operator Hazard Level” (OHL) to qualitatively assess risk. The OHL provides an approach for determining which events require mitigating action and whether the action needs to be immediate. The OHL is defined as the assessed severity an operator assigns to safety events, whether experienced or predicted, and the perceived consequences. An operator creates this OHL by reviewing historical events, generic failures, or as an alternate, using the list noted in Appendix A, to create a hazard or failure list of events that they feel warrants monitoring. The manufacturer may also be requested to provide assistance in creating this list. Once the list is created, the operator categorizes the severity of each event. The list is organized with higher severity items placed at the top and descending as the severity determination is lower.

The intention is to use the list to identify the more severe events and allocate more resources to reduce the frequency of occurrence to an acceptable level. This approach is a very basic concept compared with quantitative hazard analysis sometimes used by the manufacturers, but it provides a simple, cost effective, and time sensitive approach for the airline operator to assess risk. Its intent is to identify significant risks to the design, and the failure causes should not be sub-divided in an attempt to show that the risk is at acceptable levels. For example, reducing a fuel fire hazard from a Critical to an Acceptable risk by considering fire risk to individual components instead of considering fire risk to the overall system.

The operator-developed list contains event severities below the Catastrophic levels of the regulatory advisory material. When an event occurs at the Catastrophic level there is a regulatory oversight process that is used to identify the root cause and the necessary mitigating recommendations. The OHL intentionally places a higher emphasis on events below the Catastrophic level in the belief that if these items are resolved, it would provide immediate relief for operational events such as Rejected Takeoffs, Diversions, or Returns to the Field. If these events remain unresolved, they may ultimately become a link in a catastrophic event.

B.5.2 Hazard Risk Matrix - Severity/Probability Assessment

After a specific safety issue has been assigned a severity category and assigned a qualitative probability category, the results are compared to the organization’s formal risk criteria. A convenient way to do this is to utilize a Hazard Risk Matrix. Typically, a Hazard Risk Matrix lists the appropriate severity categories on one axis, and the qualitative average fleet probability categories on the other. Within the matrix, the organization’s formal risk criteria are listed. Thus, for each possible combination of severity and probability, the matrix lists the required response per the company’s formal criteria. An example of a Hazard Risk Matrix is shown in Table B12.

Table B12 - Hazard risk matrix example

Hazard Risk Matrix				
Risk Severity Risk Probability	Negligible	Marginal	Critical	Catastrophic
	Example			
Frequent	OK	WORK	IMMED	IMMED
Probable	OK	OK	WORK	IMMED
Occasional	OK	OK	WORK	IMMED
Remote	OK	OK	OK	WORK
Improbable	OK	OK	OK	WORK

For this example, Hazard Risk Matrix, a specific safety issue needs no action if it's classified "OK" in Table B12. If an issue receives a "WORK" classification, the organization will mandate some improvement actions to bring the issue back to an "OK" status. For a "WORK" classified issue, the organization reserves some discretion with the scheduling and priority of corrective actions. For a safety issue assessed as "IMMED," the organization will mandate some IMMEDIATE internal corrective action. Typically, this immediate action might be a forced inspection or other interim action. If the IMMEDIATE action is only an interim solution, a parallel "WORK" activity is undertaken to determine a permanent corrective action.

Note that use of a risk matrix provides a basic, simplified overview of risk that makes it easy to display and communicate. However, as it is simplified, it is important to recognize that there are nuances that are lost in the simplification process. For example, a matrix, by definition, presents changes in risk levels as step functions. This means that several orders of magnitude of probability are assigned the same risk level, but then a small change in probability represents a step change to a different risk level. If more granularity is needed, the user should consider a quantitative assessment.

Additionally, recognize that using a matrix often implies the "worst-case" or "most credible" outcome is the only risk that gets evaluated. In reality, all outcomes should be evaluated (for example, hazardous at probable as well as catastrophic at remote).

Finally, these classifications can result in an implied equivalence that does not exist. Per this example the difference between Marginal and Critical is interpreted as being the equivalent to the difference between Critical and Catastrophic. Similarly, the classifications imply that Marginal failures that occur Frequently (WORK) is equivalent to a Catastrophic failure that occurs Remotely. This can result in mis-prioritization of resources to address the various hazards.

APPENDIX C - QUANTITATIVE RISK ASSESSMENT

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

C.1 QUANTITATIVE ASSESSMENT

This appendix describes the probability calculations that support a quantitative risk assessment. Risk has two elements - severity and the probability. In a quantitative analysis, the severity level(s) of concern is evaluated for probability of occurrence. In most cases, a conditional probability is combined with the probability of an initiating event to get the probability of the severe outcome. This appendix describes the calculations that support this assessment.

C.1.1 Measurement Units

A key element in performing a risk assessment for a specific safety event is calculating a measure of the probability of occurrence. The resulting probability value is usually expressed as either probability per flight hour or probability per flight which is how probability is referenced in this document. There are also situations in aviation risk analyses where the failure mode may be a function of calendar days, rather than flight hours or flights (for example corrosion).

C.1.2 Event Probability Based on Observed Rate

Often, an airplane malfunction, failure, or defect becomes an issue after it is actually observed in service. (The issue may also be identified by new or refined analysis, anomalous findings, or other information.) The data available for a probability evaluation is then the number of observed events, and the number of flights or flight hours operated on airplanes exposed to the problem. Assuming the Rare Event Approximation described in 1.3 is applicable, the probability is equal to the observed event rate. Thus, the probability is calculated simply by dividing the number of observed events by the number of flight hours (or flights) operated by the fleet of exposed airplanes. For example, if nine fuel leak events have been observed over a service period of 450000 flight hours, the event probability per flight hour is calculated as $9/450000 = 2.0E-05$.

Note that the simple calculation above provides a single probability value. This value is then used as the probability per flight hour regardless of product age. Thus, the assumption is made that the probability of failure remains constant as the product ages. If this assumption is not reasonable- i.e., an infant mortality or wearout condition is suspected- the methods discussed in C.1.7 must be used. As a simplification, in the absence of the data necessary to estimate a non-random failure rate, the past year or two of data can reasonably estimate the risk for the next year or two.

The failure rate may need to be estimated even though no failure has occurred in service. To estimate the failure rate, a common approach is to assume that there is one imminent failure in the fleet and then divide 1 by the fleet's accumulated flights or flight-hours. Note that the assumption is for 1 imminent failure in the entire fleet, not that each airplane in the fleet has an imminent failure, the latter being so outlandishly conservative that it is unusable. Assuming 1 failure results in a failure rate estimate that is a conservative 63% confidence bound of the true failure rate (the actual 63% confidence bound could be less, even drastically less, but there is a lack of service data to know how much less). It likewise represents the failure rate "if we had an event tomorrow."

When there have been failures, and the number of failures has been divided by the accumulated flights or flight hours, the failure rate estimated is the MLE point estimate. The MLE estimate corresponds to the average expected failure rate (50% confidence bound). In order to obtain an equivalent estimate when there have been no failures, 0.693 may be assumed (Poisson distribution, 50% likelihood of zero failures). Dividing 0.693 by the accumulated flights or flight-hours results in the average expected failure rate demonstrated to date (50% confidence bound). Once again, the actual failure rate could be less, but how much less is unknown due to lack of data. Using 0.693 to determine the failure rate results in an analysis that is more consistent and comparable with other analysis where failures have occurred.

C.1.3 Rare Event Approximation

The Rare Event Approximation is used throughout this appendix, which allows probability calculations based on observed event rates to be simplified in two ways:

- a. probabilities can be approximated by dividing the number of events by the number of flight hours (or flights),
- b. when an event can occur due to multiple causes, adding the probabilities of the multiple causes approximates the probability of the event when the individual event probabilities are all 0.01 or less.

It is recognized that the Rare Event Approximation is not appropriate for probabilities greater than 0.01. For these situations, perform probability calculations using the exact method, as shown in Table C1.

Table C1 - Rare event approximation to exact comparison

	<u>Rare Event Approximation</u>	<u>Exact Method</u>
Probability per flight hour from observed data	= # Events / # Flight Hours	$= \lambda(e^{-\lambda})$ with $\lambda = \text{\# Events} / \text{\# Flight Hours}$
Probability of A or B	= Probability of A + Probability of B	$= 1 - [(1 - \text{Probability of A}) \times (1 - \text{Probability of B})]$

NOTE: Even the Exact Method formulas are valid only when certain assumptions are applicable. Using $\lambda(e^{-\lambda})$ to calculate a probability value is valid only for constant failure or event rate situations. Using the listed formula for calculating the Probability of A or B is valid only when the events are independent.

C.1.4 Confidence Bound on Observed Rate

When a probability calculation is based on a small number of observed events, the results are subject to significant statistical uncertainty. Conservatism may be added any of several ways; in the assumptions used for the risk analysis, by a risk abatement plan more aggressive than the analysis might suggest or by adding a confidence bound to the results of the analysis.

The formula shown below is applicable for events where the probability can be treated as independent of product age. The statistical assumption is that the observed events arise from a Poisson process.

$$\text{Probability} \leq [\chi^2_{\alpha, 2(r+1)}] / 2T \quad (\text{Eq. C1})$$

where:

T = total flight hours (or flights)

α = 1 - selected statistical confidence level

r = number of observed events

$\chi^2_{\alpha, k}$ = α th percentile of Chi-square probability distribution with k degrees of freedom

Application of the Equation C1 formula involves use of the chi-square distribution (χ^2), for which tables are provided in the appendices of most statistics textbooks.

For the previous example, where 9 fuel leaks were observed over 450000 flight hours, we calculate a 90% confidence bound using the parameter values:

$$T = 450000$$

$$\alpha = 1 - 0.90 = 0.10$$

$$r = 9$$

From a table of the chi-square distribution, we find that:

$$\chi^2_{0.10, 2(9+1)} = \chi^2_{0.10, 20} = 28.412$$

And so inserting into Equation C1,

$$\begin{aligned} \text{Probability} &\leq 28.412 / [2(450000)] \\ &\leq 3.157\text{E-}05 \text{ per flight hour} \end{aligned} \quad (\text{Eq. C2})$$

The value 3.157×10^{-5} is a conservative upper bound of 90% confidence on the probability. This upper bound provides a probability value appropriately adjusted for statistical uncertainty. The amount of the adjustment is a function of the sample size (i.e., nine events) and the selected confidence level (i.e., 90%). For the example of 9 fuel leaks in 450000 flight hours, the 90% confidence bound probability is greater than the observed probability by a confidence factor of 1.578 (i.e., $3.157\text{E-}05 / 2.0\text{E-}05 = 1.578$).

Note that a confidence bound on the observed probability can be calculated even when there have been no observed events. To illustrate, suppose that service experience shows that there have been zero aborted takeoffs in 100000 hours of service, and a 60% confidence level is desired.

Equation C1 is used as follows:

$$\text{Probability} \leq [\chi^2_{\alpha, 2(r+1)}] / 2T,$$

where:

$$T = 100000$$

$$\alpha = 1 - 0.60 = 0.40$$

$$r = 0$$

From a table of the chi-square distribution, we find that:

$$\chi^2_{0.40, 2(0+1)} = \chi^2_{0.40, 2} = 1.832 \quad (\text{Eq. C3})$$

And therefore:

$$\begin{aligned} \text{Probability} &\leq 1.832 / [2(100000)] \\ &\leq 9.160\text{E-}06 \text{ per flight hour} \end{aligned} \quad (\text{Eq. C4})$$

Just as before, the value $9.160\text{E-}06$ can be interpreted as a conservative upper bound on the probability. This upper bound provides a probability value appropriately adjusted for statistical uncertainty.

Table C2, below, provides confidence factors for sample sizes of 1 to 10, for confidence levels of 75%, 90%, and 95% for a Poisson process. These confidence factors can be used directly to convert observed probabilities to upper bound probabilities to appropriately account for statistical uncertainty.

Table C2 - Confidence factors to adjust observed probability

<u>Sample Size</u>	<u>75% Confidence</u>	<u>90% Confidence</u>	<u>95% Confidence</u>
1	2.693	3.890	4.744
2	1.960	2.661	3.148
3	1.703	2.227	2.585
4	1.569	1.998	2.288
5	1.485	1.855	2.192
6	1.426	1.755	1.974
7	1.384	1.682	1.878
8	1.350	1.624	1.804
9	1.324	1.578	1.745
10	1.302	1.541	1.696

As an example, if two false fire warnings were reported over a period of 400000 flight hours, the observed probability is calculated as $2/400000 = 5.0\text{E-}05$ per flight hour. For 90% confidence and a sample size of 2, the confidence factor from the table above is 2.661. Therefore the 90% confidence upper bound probability is $(2.661) \times (5.0\text{E-}06) = 1.331\text{E-}05$ per flight hour.

For confidence levels and/or sample sizes not listed in the table above, the confidence factor can be calculated using the formula presented in Equation C5.

$$\text{Confidence Factor} = [\chi^2_{\alpha, 2(r+1)}] / 2r \quad (\text{Eq. C5})$$

where:

α = 1 - selected statistical confidence level

r = number of observed events

CAUTION: Confidence factors when applied to a single event provide appropriate conservatism, but can lead to excessive conservatism when applied to multiple events in combination as covered in C.1.5 and C.1.6. Additionally, be especially careful when comparing and prioritizing risks. Choosing to prioritize on the basis of (for example) the 90% confidence prediction rather than the average prediction could lead to prioritizing a low-risk issue with few events (and thus a large confidence band) over high-risk issue with many events (and thus a tight confidence band). Remember also that the confidence band is not uniform; the true value is more likely to be close to average than to the far extent of the confidence band. Finally, the true answer is as likely to be below the average as it is to be above.

C.1.5 Predicted Event Rate Based on Observed Rate of Contributing Elements

As a general rule, nearly all accidents and airplane hazardous events arise not from a single cause, but from a combination of two or more causes or contributing elements. Typically, it is the occurrence of one of these contributing elements that has triggered the need for a risk assessment, rather than the occurrence of a hazardous event. In these cases, the observed contributing element should be reviewed in the context of the potential hazardous event.

Consider this simple example. Although fuel leaks are always a concern, they become even more serious if the fuel comes into contact with an ignition source. Typically, basic airplane design incorporates physical barriers to separate potential fuel leak areas from potential ignition areas. In principle, therefore, a fire can occur only if a fuel leak occurs and there is a failure (e.g., shorted wire) or malfunction which provides an ignition source.

In the previous example, where nine fuel leaks were observed in 450000 hours, an observed probability of $2.0\text{E-}05$ was calculated. To expand the example, let's assume that, over the same 450000 flight hours, five shorted wires and two engine over-temperature malfunctions were observed that could result in an ignition source for fuel. Therefore, there were a total of seven observations of potential ignition sources over this period. This provides an observed ignition source probability of $7/450000$ hours = $1.556\text{E-}05$ per flight hour.

Since a fire can occur only if a fuel leak and an ignition source occur concurrently, the probability of a fire can be calculated as the product of the two contributing probabilities (assuming that fuel leak and ignition sources are independent events).

$$\text{Probability of Fire} = \text{Probability of Fuel Leak} \times \text{Probability of Ignition Source} \quad (\text{Eq. C6})$$

$$= 2.0\text{E-}05 \times 1.556\text{E-}05 = 3.112\text{E-}10 \text{ per flight hour}$$

C.1.6 Accounting for Latent Failures

A latent (dormant) failure mode is a failure that is not apparent to the flight crew or maintenance crew, and therefore remains in a failed state for multiple flights. When a latent failure mode is a contributing element to a safety event, the probability of the safety event is higher because of the latency. From the example above, there were five occurrences of shorted wires. These occurrences were discovered during the daily electrical system check, and thus could have become shorted anytime during the previous day. If the typical airplane in the affected fleet operates 8 hours per day, and a daily inspection is used to check for shorted wires, the potential latency period for the wire is 8 hours. This means that a shorted wire could be in service for as little as zero hours or as long as 8 hours. The average exposure period for this simple example is approximated as half of the total 8 hour latency exposure time, or 4 hours.

To account for latency, the probability of having a shorted wire is calculated as the product of the observed occurrence rate and the average exposure period. Continuing with the same example, there were five occurrences of shorted wire in 450000 hours, and the average exposure period is 4 hours. Therefore:

$$\text{Probability of Shorted Wire} = [5 / 450000] \times 4 = 4.444\text{E-}05 \text{ per flight hour} \quad (\text{Eq. C7})$$

Assuming that the other "contributing elements" are not latent:

$$\text{Probability of Over Temperature} = [2 / 450000] = 4.444\text{E-}06 \text{ per flight hour} \quad (\text{Eq. C8})$$

$$\text{Probability of Fuel Leak} = [9 / 450000] = 2.0\text{E-}05 \text{ per flight hour} \quad (\text{Eq. C9})$$

Since an ignition source can result from either a shorted wire OR an over temperature condition:

$$\begin{aligned} \text{Probability of Ignition Source} &= \text{Probability of Shorted Wire} + \text{Probability of} \\ \text{Over Temperature} &= 4.444\text{E-}05 + 4.444\text{E-}06 \quad (\text{Eq. C10}) \\ &= 4.889\text{E-}05 \text{ per flight hour} \end{aligned}$$

Since a fire can result only if both a fuel leak AND an ignition source is present:

$$\begin{aligned} \text{Probability of Fire} &= \text{Probability of Fuel Leak} \times \text{Probability of Ignition Source} \quad (\text{Eq. C11}) \\ &= 2.0\text{E-}05 \times 4.889\text{E-}05 \text{ per flight hour} \\ &= 9.778\text{E-}10 \text{ per flight hour} \end{aligned}$$

Note that in the previous example, only one failure mode is potentially latent. For this case, an exposure period equal to one-half of the latency period can be used. However, for cases where more than one failure mode may be latent, the calculation is more complicated. This is described in ARP4761, Fault Tree and Markov Appendices as average probability calculation methodology.

C.1.7 Accounting for Component Aging Characteristics (Weibull Analysis)

Up to this point, the results of probability calculations have been expressed as a single probability value. This value is then used as the probability per flight hour (or per flight) regardless of product age. Thus, the assumption is made that the probability remains constant as the product ages. When this assumption is not reasonable, i.e., an infant mortality or wearout condition is suspected, probability calculations can be based on the results of a Weibull analysis or other failure distribution analysis.

Appendix E provides a detailed description of Weibull analysis. In this document, the results of a Weibull analysis will be used to calculate probability per flight hour (or flight) values.

To illustrate using the earlier example of nine fuel leaks in 450000 hours, assume that further investigation found that the leaks were all due to fatigue failures of a specific fuel tube fitting. It was suspected, and then confirmed through Weibull analysis, that the fatigue failures exhibited wearout, meaning that higher age fittings were more likely to fail than lower age fittings. Specifically, Weibull analysis indicated a Weibull slope (shape parameter) of 2.3 and a characteristic life of 30000 hours.

A review of the in-service fleet found that the highest time fuel tube fitting had been in operation for 25000 hours. Since the Weibull distribution indicates a wearout condition, the 25000-hour fitting has a higher failure probability than the lower-age fittings in the fleet. Of particular interest, in this case, is quantifying the failure probability (per hour) of this specific fitting. This probability is equivalent to the hazard rate at 25000 hours, which can be calculated from Equation C12.

$$h(t) = (\beta/\eta) (t/\eta)^{(\beta-1)} \quad (\text{Eq. C12})$$

where:

$h(t)$ = hazard rate at time t

β = Weibull slope (shape parameter)

η = Weibull characteristic life

t = selected component age

For the example above:

$$\begin{aligned} h(25000) &= (2.3 / 30000) (25000 / 30000)^{(2.3 - 1)} \\ &= 6.049\text{E-}05 \end{aligned} \quad (\text{Eq. C13})$$

This hazard rate, 6.049×10^{-5} , represents the probability of failure (per hour) for a fitting with 25000 hours of operation. Note that this is about three times higher than the fleet average probability of 2.0×10^{-5} which was calculated earlier. This further illustrates the aging or wearout characteristic of the fitting.

To further expand the example, Table C3 shows calculation results for fittings with ages varying from 5000 to 30000 hours.

Table C3 - Example results for varying ages

<u>Fitting Age (hours)</u>	<u>Fitting Failure Probability (per hour)</u>
5000	7.465E-06
10000	1.838E-05
15000	3.114E-05
20000	4.526E-05
25000	6.049E-05
30000	7.667E-05

C.1.8 Accounting for Multiple Contributing Elements (Monte Carlo Analysis)

In the previous discussion and examples, probability assessments were based on analysis of observed failure data. There are times when additional information is available that can be used to develop a more complete model of the failure mode. As an example, failure of an engine turbine disk can be a function of:

- a. Cycles to initiation of a crack
- b. Location of the crack
- c. Crack propagation rate
- d. Frequency of inspection opportunities
- e. Inspection efficiency
- f. Disk retirement age

If through engineering analysis, test data or other means, information on the above parameters can be established, Monte Carlo Simulation can be used to calculate the probability of a turbine disk failure. See Appendix F for details on performing Monte Carlo Analysis.

C.2 FLEET RISK ASSESSMENT

C.2.1 Measurement Units

Fleet risk assessment is essentially an application of the probability evaluation described earlier to an entire fleet. Where the earlier calculations provided probabilities on a per flight hour or per flight basis, the results of a fleet risk assessment are typically expressed as total events for the fleet versus calendar time, or total events for the fleet until fleet retirement or problem elimination.

C.2.2 Prediction Based on Observed Event Rates

As mentioned earlier, when probability calculations are based on observed event rates, there is an inherent assumption that the contributing events are random in nature. That is, the risk for an individual airplane is not affected by the age of the airplane or the airplane components. So each airplane, regardless of its age or history, has an identical risk when expressed on a per flight hour or per flight basis.

When the risk for an individual airplane can be considered constant, and the risk for each airplane in the fleet can be considered equal, the fleet risk is a function only of the individual airplane risk and the period of time that the fleet is exposed to that risk. As an example, consider a case where a fuel pump problem has been identified which can lead to an engine shutdown. For this example, using the procedures of Section C.1, the risk of an engine shutdown has been calculated to be 5×10^{-6} per engine flight hour. If the fleet consists of 500 airplanes, each with two engines, and each operating 8 hours per day, the fleet operating time for one day is equal to (Equation C14):

$$(500 \text{ airplane}) \times (2 \text{ engines/airplane}) \times (8 \text{ flight hrs per day/engine}) =$$

$$8000 \text{ engine flight hours per day} \quad (\text{Eq. C14})$$

If a corrective action plan is to be implemented at a rate of 50 airplanes per month over a 10-month period, the average exposure per airplane is 5 months. Thus the total fleet exposure to the fuel pump problem is:

$$(5 \text{ months}) \times (30 \text{ days/month}) \times (8000 \text{ engine flight hours/day}) =$$

$$1200000 \text{ engine flight hours} \quad (\text{Eq. C15})$$

The fleet risk, expressed as the expected fleet event count, is then:

$$(5\text{E-}06 \text{ events/engine flight hour}) \times (1200000 \text{ engine flight hours}) =$$

$$6.0 \text{ events} \quad (\text{Eq. C16})$$

Thus, if the corrective action plan is implemented according to the proposed schedule of 50 airplanes per month, six engine shutdown events can be expected before the entire fleet is corrected.

C.2.3 Accounting for Component Aging Characteristics (Weibull Analysis)

In C.2.2, the assumption is made that the probability of failure remains constant as the product ages. When this assumption is not reasonable, i.e., an infant mortality or wearout condition is suspected, probability calculations can be based on the results of a Weibull analysis or other failure distribution analysis. This is described in C.1.7, and with more detail in Appendix E.

A Weibull analysis (or other failure distribution analysis) will quantify the aging characteristics of the applicable component failure mode. The fleet risk can then be calculated as a function of (1) the assessed Weibull distribution, (2) the specific age (known or estimated) of each product in the fleet, and (3) the planned corrective action schedule.

C.2.3.1 Calculating Approximate Fleet Risk Using a Simplified Method

As an example, consider the fuel tube fitting problem of C.1.6. The C.1.6 analysis provided Table C3, which defines the fitting failure probability as a function of fitting age.

The fleet consists of 20 airplanes, each with one of the specific fuel tube fittings of concern. The 20 fuel tube fittings in service have various ages and, consequently, various failure probability values. The fleet risk calculation then looks at each fitting individually, and multiplies that fitting's risk per hour value, times the expected future service time until corrective action (or fleet retirement). This provides an expected failure probability, for each individual fitting, for the remaining service time until corrective action is taken (or fleet retirement). A sum of these values provides the fleet risk, expressed as the expected event count, until the entire fleet is corrected. Table C4 illustrates this procedure. Notice that the individual fittings have been grouped by age to simplify the calculation. Also notice that the corrective action plan, for this example, provides more rapid implementation for the higher time fittings. This approach, of course, reduces the fleet risk compared to a more arbitrary schedule, which ignores the component aging characteristic.

The fleet risk value of 0.6183 can be interpreted as the expected event count for the entire fleet during the corrective action period.

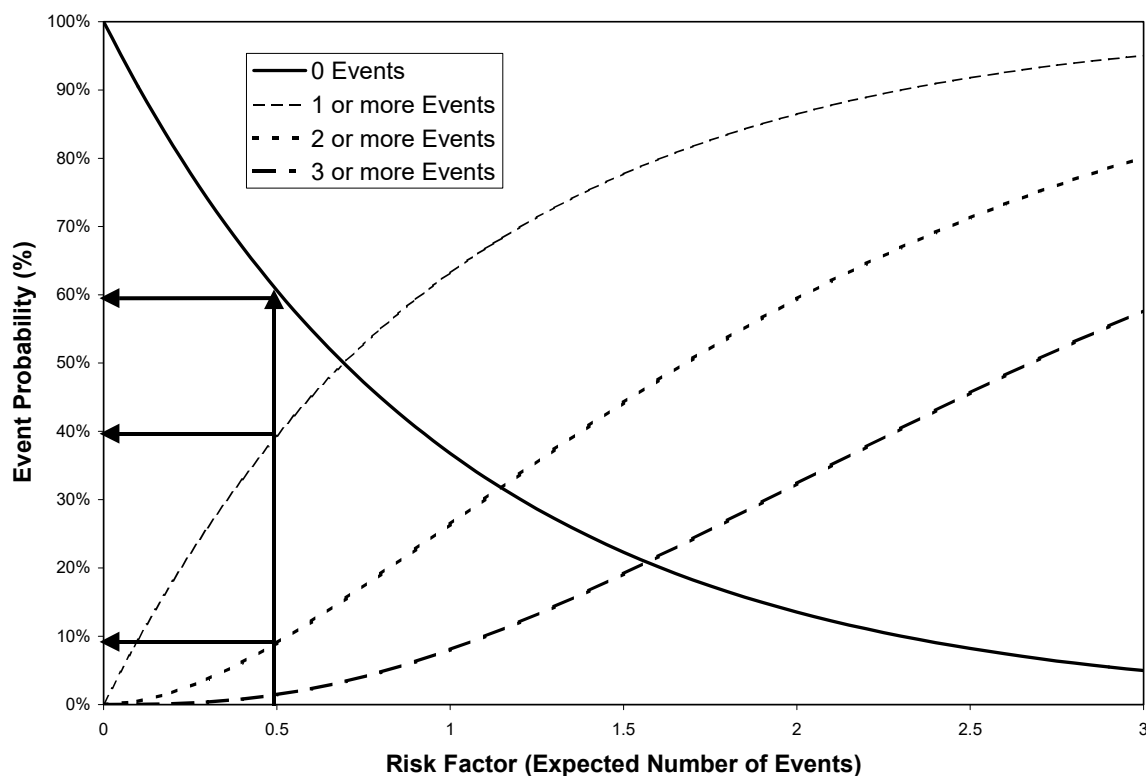
Table C4 - Cumulative fleet risk illustration

Fitting Age <u>A</u>	Quantity of Fittings in Service <u>B</u>	Fitting Failure Probability (per hour) <u>C</u>	Planned Service Time Until Corrective Action <u>D</u>	Cumulative Risk Value for Group B x C x D <u>E</u>
5000	5	7.465E-06	2000	0.0747
10000	4	1.838E-05	2000	0.1470
15000	3	3.114E-05	1000	0.0934
20000	3	4.526E-05	1000	0.1358
25000	3	6.049E-05	500	0.0907
30000	2	7.667E-05	500	0.0767
Fleet Risk = Sum of Column E values				0.6183

The risk analyst may be asked to relate the fleet risk value in terms of event probability. Figure C1 shows that relation. So if the risk analyst has a (for example) fleet risk of 0.50, there is a 60.7% chance of no failure events occurring, a 39.3% chance of one or more, a 9% chance of two or more, etc. This is arrived at by using the Poisson formula with the mean value (λ) equal the fleet risk. Thus, if fleet risk is denoted by the symbol β , then:

$$P(\text{Event Count} = N) = e^{(-\beta)} \beta^N / \text{Factorial}(N)$$

Thus $P(\text{Event Count} = 0) = e^{(-0.5)} = 0.607$ (a 60.7% chance of no events) and so on.

**Figure C1 - Event probability versus fleet risk**

APPENDIX D - ROOT CAUSE (EVENT TREE) ANALYSIS

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

D.1 SCOPE

Three main tools are used in the standardized root cause analysis: (a) the event tree, (b) the root cause disposition chart, and (c) the action item list. The tools are straightforward, easy to understand and use, and provide a clear structure to follow for the investigation. If complete, the tools will also provide full documentation of the evidence collected and deduced throughout the failure investigation.

D.1.1 The Event Tree

The event tree has a structure similar to a fault tree, but without the use of logic gates. It serves as a visual depiction of all plausible events, which may occur to cause the top undesired event. A generic event tree is pictured in Figure D1. The top event is usually the most clearly identifiable direct effect, which is being investigated, such as "blade fracture," or "disk liberation." However, if little is known about how the failure occurred, the top event may be as broad in scope as "airplane loss." The next level of events consists of all plausible events, which may cause the top event. Each event on that level is then examined for all plausible events, which may cause that event. The tree then "grows" as each event is evaluated for its potential causes. The lowest level of events, for which there are no further causes, comprise the set of root causes for the top event. Each root cause is considered a potential contributor to the failure, and root causes are understood not to be mutually exclusive. In this way, no single root cause must be the only cause for the top event; several root causes may act together to cause the top event. The path that each root cause traces to the top event represents a potential scenario for the failure, where following the path from the top event to the root cause shows causal relationships, and following from the bottom root cause to the top event shows effectual relationships.

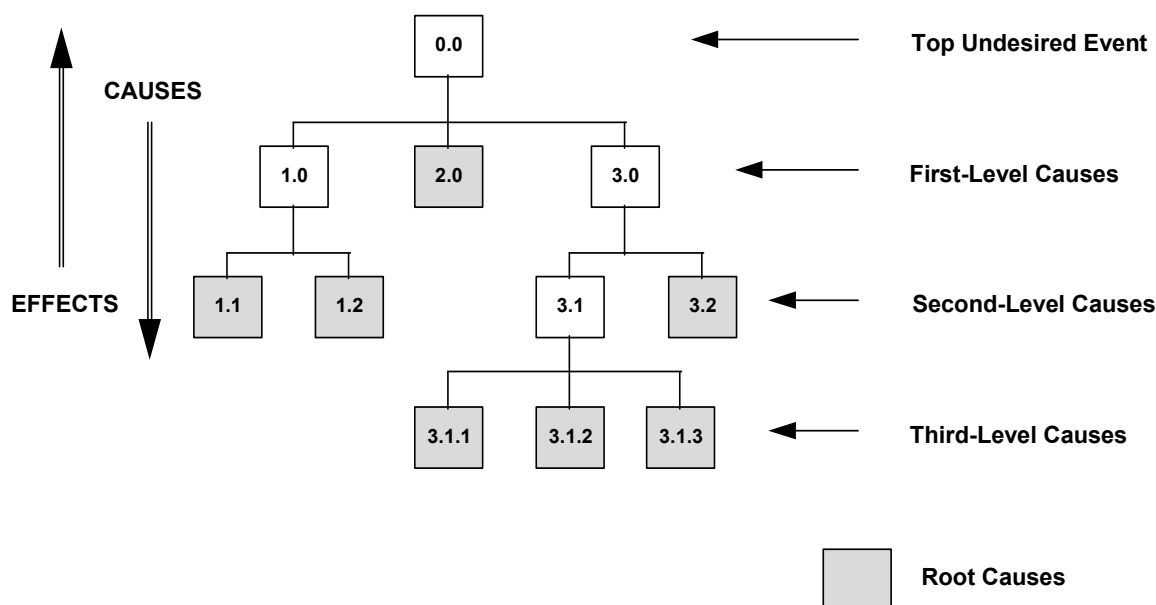


Figure D1 - Generic event tree

The event tree serves several purposes. It gives the investigation team a clear picture of all plausible scenarios for the failure, including how each scenario develops to cause the top event. The event tree shows cause-effect relationships to aid in the investigation of the real root causes of the failure, rather than intermediate effects. Branches of the event tree can be shaded or colored to show prioritization of root causes for investigation or root cause closure status to be presented to management or the customer. The structure of the event tree may be used to break the investigation team into sub-teams, each of which is responsible for researching and dispositioning a section of the event tree. The event tree also provides a visual aide for presentation of the results of the investigation, where the most probable scenarios can be clearly traced.

D.1.2 Root Cause Disposition Chart

Disposition charts are used to track all known data and action items regarding each event, including potential root causes in the event tree. For each event and root cause, there will be evidence supporting and/or refuting how that event contributed to the failure. This data may apply specifically to a root cause, or it may apply more generally to a higher level event in the tree. As the investigation progresses, supporting and refuting data will be added to the disposition chart, and an assessment may be made at any time as to whether enough evidence exists to close each event as one, which did or did not contribute to the failure. If existing data is not sufficient to make a decision as to the contribution of the event, then an action item must be assigned to gather more data. The status of each action item and the priority of the event are indicated on the disposition chart.

A standard format for the disposition chart is shown in Table D1.

Table D1 - Root cause disposition chart format

<u>Event #</u>	<u>Event Description</u>	<u>Supporting Evidence</u>	<u>Refuting Evidence</u>	<u>Action Description</u>	<u>AI #</u>	<u>AI Status</u>	<u>Event Priority</u>
Number of each event and root cause on the event tree	Title of each event and root cause on the event tree	Evidence which supports this event as a contributor to the top event	Evidence which does not support this event as a contributor to the top event	Description of action item assigned to gather more evidence for this event	Number assigned to action item	Status of action item (Proposed, Not Started, Working, Complete)	Relative priority assigned to event (Probable, Unlikely, Closed)
Example:	-----	-----	-----	-----	---	-----	-----
1.1.1.1	Incorrect material composition		XES examination confirmed correct alloy type for blade from incident engine #1	Perform XES examination of blade from incident engine #1 to confirm proper material composition	12	Complete	Unlikely

D.1.3 Action Item List

The full listing of action items ties in to the action items listed on the disposition chart. It allows for more information to be provided, including the responsible actionee, the due date, and a list of other root cause numbers, which the action may also address. The action item list is in a spreadsheet which may be sorted by root cause numbers, actionee, or due dates. This list provides a method of managing the work being done to support the investigation, coordinating activities, allocating resources, and estimating completion or disposition dates. Actions outside of the root cause investigation effort, such as corrective actions, may also be listed and tracked on the master action item list.

A standard format for the action item list is shown in Table D2.

Table D2 - Action item list format

<u>AI #</u>	<u>Cause #</u>	<u>Group/Team</u>	<u>Actionee</u>	<u>Suspense Date</u>	<u>Status</u>	<u>Action Description</u>
Number assigned to action item	Event tree event number which action item addresses	Group or team of which actionee is a member	Responsible investigation team member	Projected completion date of action item	Status of action item (Proposed, Not Started, Working, Complete)	Description of action item, including description of how it addresses the event in the event tree
Example: 12	----- 1.1.1.1	----- Materials Engineering	----- John Doe	----- 3/2/94	----- Complete	----- Perform XES inspection to confirm material composition of incident blade on engine #1

D.2 ROOT CAUSE ANALYSIS PROCESS

The root cause analysis process flow diagram is pictured in Figure D2. It is an iterative process, where each of the tools is used, and the data is re-evaluated for all iterations. The potential causes of the failure are identified by the event tree, and existing supporting and refuting data are reviewed. An assessment of the potential contribution of the cause is made, and the cause is either dispositioned as closed, or an action item is assigned to gather more data. Ultimately, when no more root causes can be eliminated as non-contributors, one or more root causes will remain as the key contributors to the failure.

This process may be applied to any investigation. Based on the priority of the investigation and the resources available to the team, an appropriate scope and level of detail may be applied when using the tools, as well as when deciding upon the organization of the team.

D.2.1 Investigation Team Organization

Depending on the magnitude of the investigation, it may be beneficial to divide the investigation team into sub-teams, each of which is responsible for investigating and dispositioning a section of the event tree. The sub-team members will then meet independently to determine what data is needed to investigate each root cause within their section of the event tree. The sub-team members will gather data on each root cause by performing the analyses themselves, or by consulting with a team of specialists assembled for the investigation. When the sub-team members conclude that sufficient data has been gathered to disposition a root cause, they will present it to the complete investigation team for review and closure concurrence. All investigation team members must be in agreement on root cause closure.

This team organization has the advantage of ensuring that each root cause has a focal point that will pursue it until it has been dispositioned. This also helps divide the work of the root cause investigation and documentation among the team members. There are disadvantages, however, if the efforts of the sub-teams are not well coordinated. Poor communication among sub-teams concerning planned action items may result in duplication of effort or inundation of the specialists with similar questions on similar issues. Dispositioning root causes by the sub-teams may also inadvertently exclude examination of interactions between root causes. Thus, issues such as these must be discussed and coordinated by the overall investigation team. In short, the role of the sub-team is to decide what data must be gathered and when sufficient data exists to disposition each root cause, and the role of the overall investigation team is to coordinate the efforts of the sub-teams.

This type of team organization may not be efficient for smaller investigation efforts, where too many of the sub-teams would consist of common team members. The sections which follow describe how each of the root cause analysis tools may be applied by either a small investigation team, or by the team/sub-team organization.

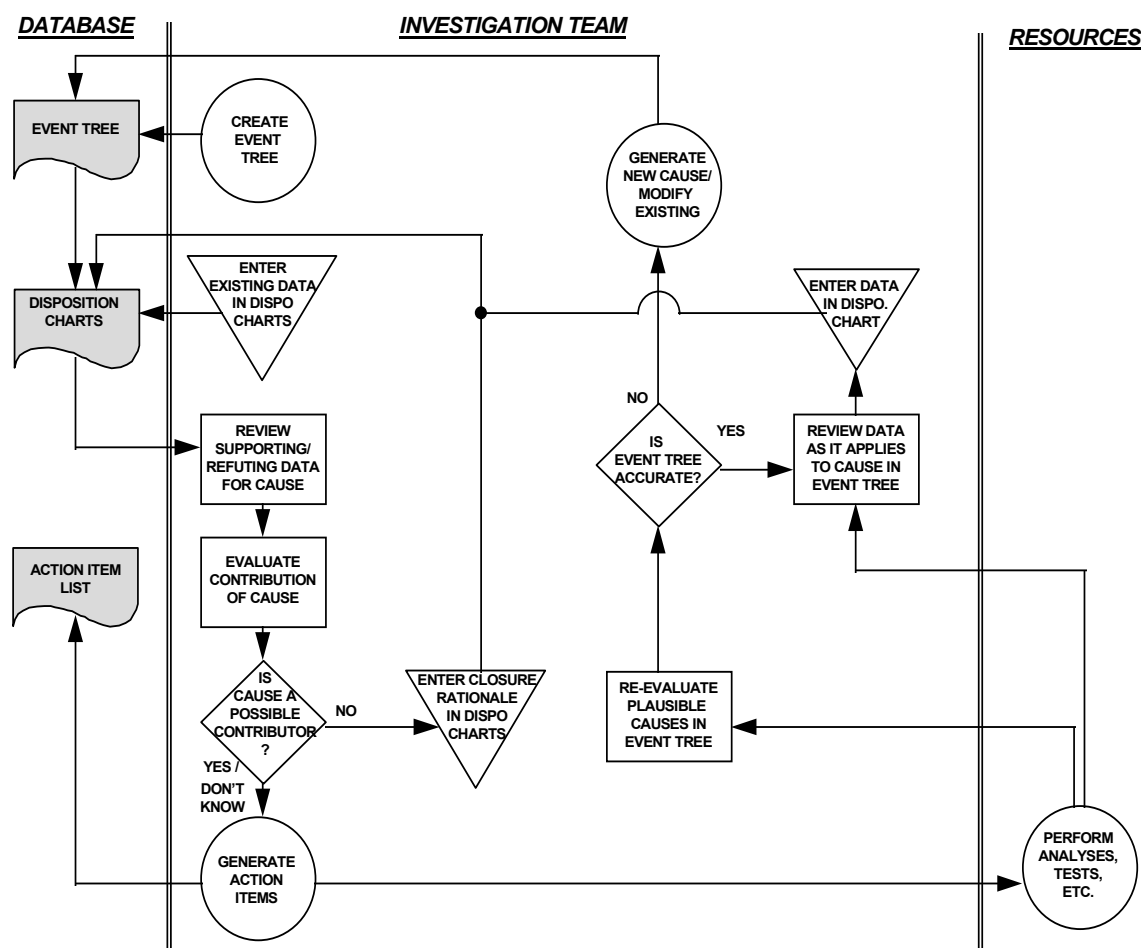


Figure D2 - Root cause analysis process flow diagram

D.2.2 Building the Event Tree

The event tree is generated from a brainstorming session with all key personnel who may provide information about the safety event being investigated. This is often an Integrated Product Development (IPD) type team with one person selected as the facilitator for the brainstorming and event tree construction. The first step is to agree on the top undesired event, usually the most readily apparent cause of the incident, if it is known. The top event should be as specific as possible, based on existing evidence about the failure. Narrowing the investigation to a specific type of failure early in the process allows the efforts of the team to be concentrated on the true issue at hand. However, if insufficient evidence exists to narrow the scope of the investigation during the initial construction of the event tree, collection of supporting and refuting data will lead to that end later in the investigation and will avoid overlooking a potential contributor to the failure. The general rule which applies to construction of the entire event tree is that if there is any doubt as to its role in the failure, it should be included in the event tree, and may be closed as a noncontributing event once concrete refuting evidence has been established.

Once the team agrees on the top event, each level on the event tree is generated by brainstorming all plausible causes of each event on the level above. This includes not only those causes which are believed to be potential contributors, but also causes for which there is currently no supporting evidence or for which there is existing refuting evidence. Those causes that are believed not to be contributors may be left at a high level, and can be closed upon formal documentation of the refuting evidence. If it is later determined that the refuting evidence is not sufficient to close the event, it may be developed in greater detail at that time. Events, which may be excluded from the event tree are scenarios that physically could not occur because of the configuration of the system. Including all plausible causes for each event will result in construction of a complete event tree, which will fully document the rationale behind the contribution of each potential scenario. It also results in an event tree, which may apply to other similar failure investigations, rather than the investigation of a specific occurrence. It may be useful to assemble a library of these event trees, which can be referenced as a starting point for future investigations or for development of design constraints for future design efforts.

It is important that the smallest possible "steps" should be taken between levels when brainstorming the causes of an event on the event tree, such that as much detail as possible is included about how the failure occurred. This will not only clarify the details of the failure, but it also aids in the brainstorming process by giving intermediate steps to the failure from which to build other scenarios. An example of this appears in Figure D3. In the example, a potential scenario for the cause of the blade fatigue fracture is misassembly of an upstream vane. If this is proposed as a first-level cause of the fracture (Figure D3A), it leaves out all the steps about how the upstream vane actually caused the blade to fail (Figure D3B). While both examples include misassembly of an upstream vane as a root cause, the latter example presents more information about the failure mechanism and helps to generate other ideas for potential causes of how the blade failed.

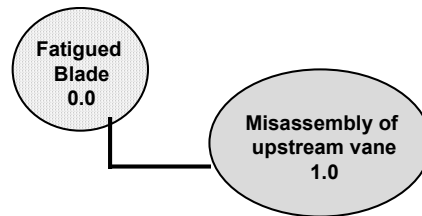


Figure D3A - Few steps to the root cause

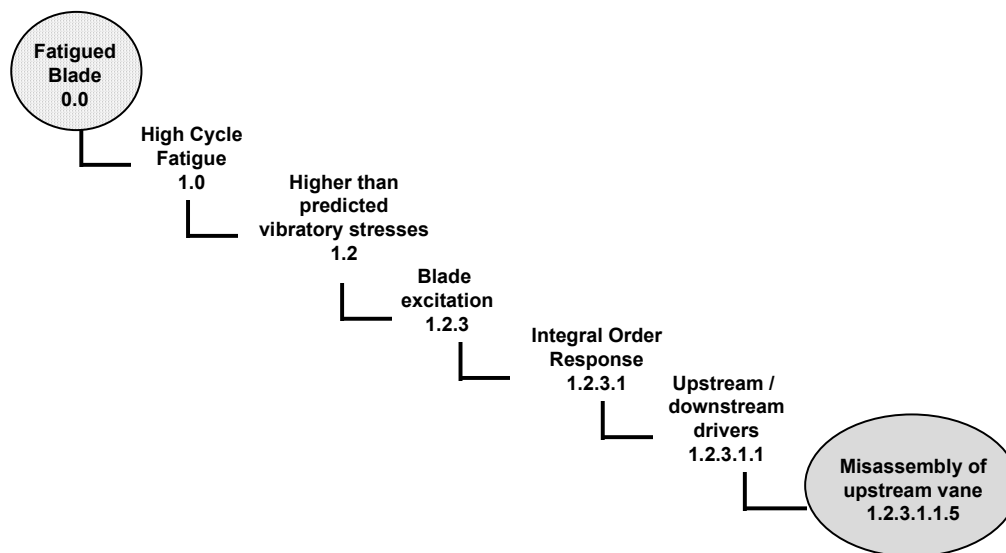


Figure D3B - Many steps to the root cause

Figure D3 - Two examples of constructing an event tree

Another way of adding meaningful detail to the event tree is to provide concise but complete descriptions for each event. Each event should be stated as a description of its magnitude and polarity (e.g., too much versus not enough) as it would contribute to the failure. For example, instead of stating an event as "*Steady Stresses*," it should be stated as "*Higher than Predicted Steady Stresses*." This provides the information that the only steady stresses which are of concern are those that are greater than those used in the blade design margins.

The event tree "grows" by continuing to brainstorm the potential causes of each event listed on each level of the tree. The event tree may be developed to the appropriate level of detail for the investigation. When it is not possible to identify any more potential causes for events on the tree, the set of potential root causes to be investigated have been produced. Root causes are defined as the lowest level of events on the event tree, regardless of the level at which they occur. For example, root causes may occur at the 4th, 10th, and 2nd levels on one event tree on different branches; each branch need not be developed to the same level as the other branches on the tree.

It should be understood that the event tree is a working document, and will continue to evolve as the investigation progresses. Invariably, the team will learn more about the failure mechanism as information is gathered, which may result in the addition of more potential causes on the event tree. Generally, events are not deleted from the event tree; they are closed out with concrete refuting evidence as non-contributors to the failure.

Figure D4 depicts the first four levels of an event tree, which was constructed to address a rotor blade fracture. The top event was selected as "0.0 Fatigued Blade," which narrowed the scope of the investigation to only the causes of fatigue failure. This was selected as the top event because the most apparent cause of the engine incident had been determined to be fracture of the blade, and a fractographic examination of suspect blades confirmed fracture in fatigue. Once the top event was agreed upon, it was determined that a fracture in fatigue could potentially be caused by any of three types of fatigue; 1.0 *High cycle fatigue (HCF)*, 2.0 *Low cycle fatigue (LCF)*, and 3.0 *HCF/LCF interaction*, which comprised the first level causes of the top event. While there was evidence which substantiated HCF, there was also evidence which refuted LCF and HCF/LCF interaction as contributing to the blade fracture. Thus it was decided to develop more detail on the HCF branch, while leaving LCF and HCF/LCF interaction to be closed out by the existing data. This provided a more complete depiction of the event tree (by including LCF and HCF/LCF interaction), while still concentrating the effort on the more probable causes.

ROTOR BLADE EVENT TREE

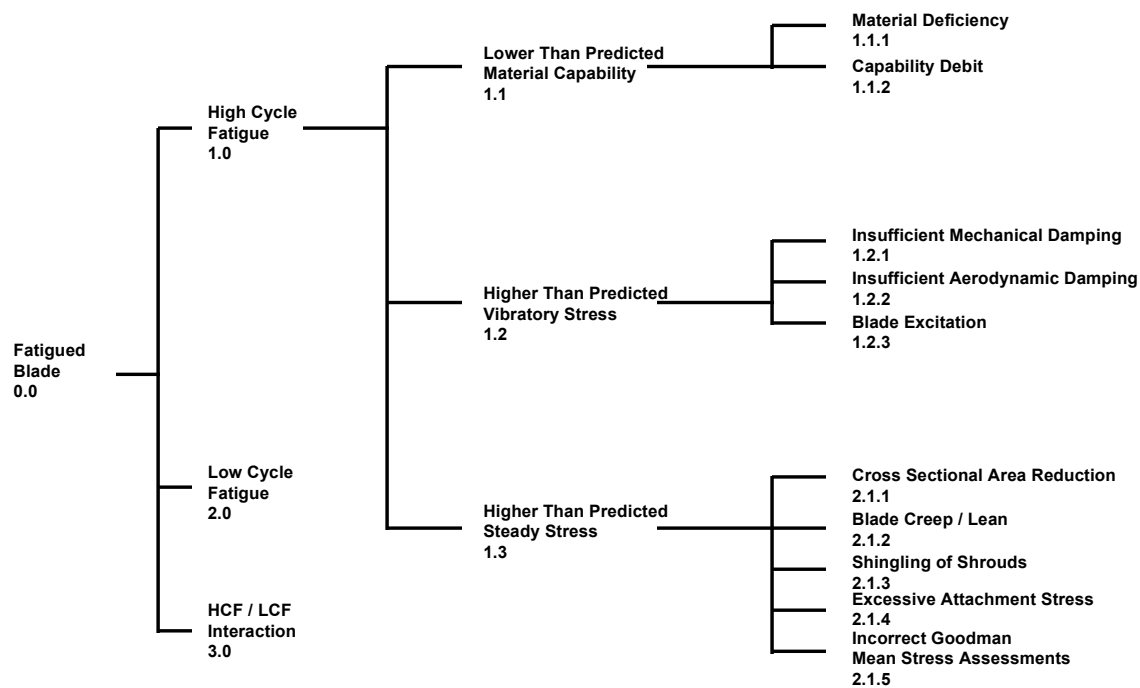


Figure D4 - Example event tree

The next level of causes in the example event tree, 1.1 Lower than predicted material capability, 1.2 Higher than predicted vibratory stresses, and 1.3 Higher than predicted steady stresses, are based on a Goodman diagram (see Figure D5). This provides the mechanical principles for why the blade fractured in HCF, where fracture of the part would occur if any individual or combination of three criteria were met; the vibratory stresses were higher than expected, the steady stresses were higher than expected, or the material properties were lower than expected. Structuring the event tree based on mechanical principles lends itself well to explaining how or why the failure occurred, and helps clarify ideas as to the cause of the failure.

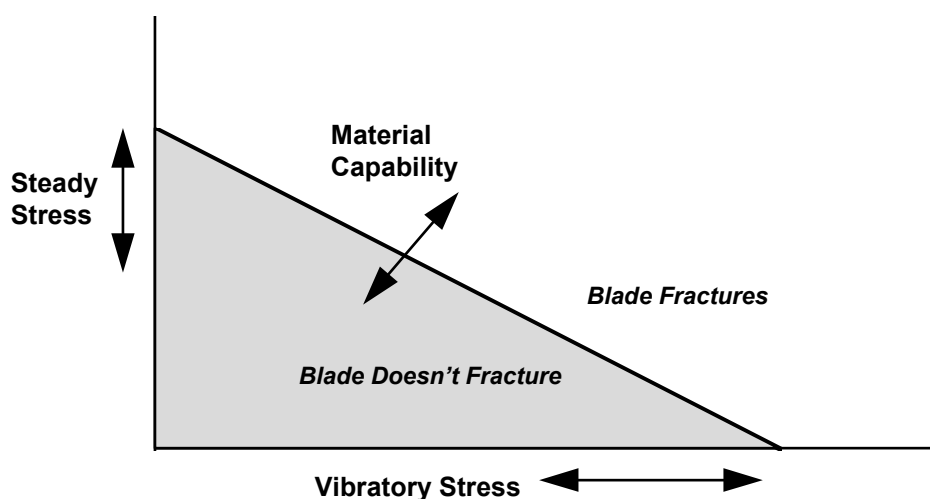


Figure D5 - Goodman diagram used in event tree

Further causes were developed in the same manner down each branch of the event tree, until (a) no more causes of each event could be determined, or (b) enough refuting evidence was already known about a cause that it could potentially be closed as not contributing to the failure. Once the initial event tree was complete, the investigation continued by establishing priorities for the ensuing work.

D.2.3 Establishing Priorities

While a truly unbiased root cause analysis should give equal effort to every root cause on the event tree, typical time and resource constraints in a failure investigation generally prevent this from occurring. It is likely that some root causes will be much easier to refute or be much less likely to have occurred based on the available evidence. Thus, as long as each root cause is addressed to a degree mutually acceptable to the investigation team members and management, it may be advantageous to initially set priorities on which root causes will be investigated with the most effort, realizing that priorities may change as more information about the failure mechanism is gained. This initial setting of priorities may be done by having the team members informally discuss each root cause on the event tree, and use their technical expertise and knowledge of the existing evidence to agree upon the root causes, which are the most likely contributors to the failure.

Each root cause may be assigned a preliminary priority of "Probable," "Unlikely," or "Proposed Closed" (root causes may only be closed by examination of the refuting data and consensus of the team). Once the priority of the root causes has been determined, the rest of the event tree priorities are assigned by flowing up the highest root cause priority to the branch. The next level branches are then assigned the highest priority flowed up from each of their subordinate branches. This is illustrated in Figure D6. Note that the top event will always have the highest priority assigned to any of its root causes.

The root cause disposition chart is created at this time to assess the existing supporting and refuting data on each root cause, and to indicate where action items need to be assigned to gather more data. If all existing supporting or refuting evidence is listed for a specific root cause, and it is not readily obvious to the investigation team members that the root cause did or did not contribute to the failure, it is an indication that further evidence needs to be gathered.

As each root cause is examined for suggested action items, consideration should be given to limited resources, such as test rigs, destructive inspections, etc. to ensure that they are properly scheduled to gather a maximum of data. The "Proposed" or "Not Started" status may be used to track action items for which resources are not yet available. This will allow the action item to be entered on the list so that it is not overlooked, but does not require it to be performed if it is later deemed not necessary.

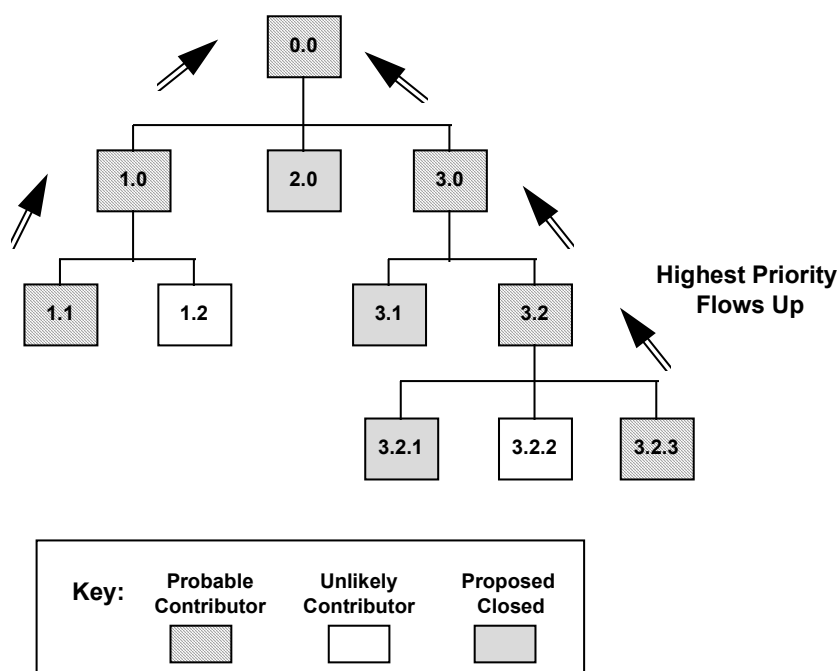


Figure D6 - Assigning priorities

D.2.4 Gathering and Tracking Evidence

Once action items are assigned, each actionee should gather the requested data as it specifically applies to the root cause where it appears in the event tree. This is necessary because each root cause traces a unique path to the top event, and different branches on the event tree represent different causes of the failure. Although the event tree may contain identical descriptions of a root cause in two different branches of the tree, they may mean different things in different branches. In the example in Figure D7, the root cause *Insufficient Assessment of Operating Conditions* appears in the *Incorrect Goodman Vibratory Assessment* branch, as well as the *Incorrect Goodman Mean Stress Assessment* branch. In the former, the root cause refers to an assessment of operating conditions when the blade vibratory design margins were being determined, while in the latter, the root cause refers to an assessment of operating conditions when the blade steady stress design margins were being determined. Although the words of the root causes are the same, they each refer to different aspects of the assessment of operating conditions.

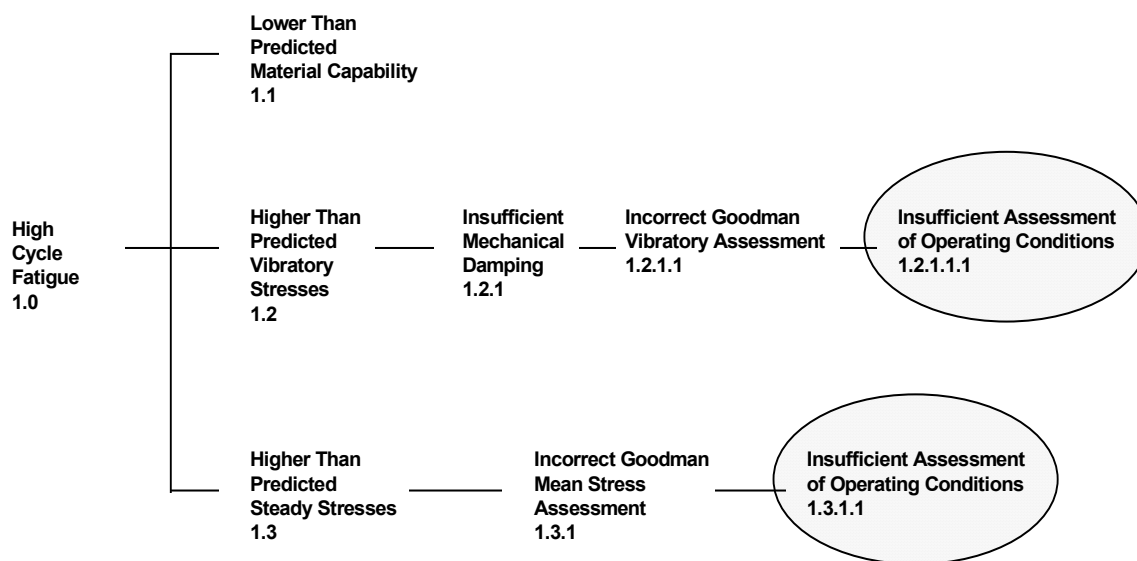


Figure D7 - Example of similar root causes

If resources allow, each root cause should be pursued as if it is suspected to be a major contributor to the failure. This will ensure that the action items assigned to it will yield as much data as possible. It is always easier to disprove the contribution of a root cause than it is to demonstrate it. Thus, if the emphasis of the investigation is to demonstrate the contribution of the root causes, they will only be closed when all attempts to demonstrate their contribution have failed. This helps ensure that important data will not be overlooked.

Data gathered and entered into the disposition chart does not necessarily have to address a specific root cause. There may be instances where the existing data addresses an entire branch of the tree. Using the rotor blade event tree example, a fractographic analysis of the fracture surface of the blade indicated a surface typical of high cycle fatigue. This data does not apply to a specific root cause on the event tree, but rather the entire *1.0 High Cycle Fatigue* branch of the tree. Thus, this evidence may influence the priorities assigned to each of the events on that branch relative to other branches of the tree which do not have this supporting evidence.

The root cause disposition chart, in conjunction with the action item list, will give an indication of the areas of the event tree which are or are not being worked. A periodic status of the investigation may be given based on the summarized information from these two sources. This will give management a rough indication of the progress of the investigation, and will allow the investigation team to track its progress relative to its goals. Two examples of status presentations are shown in Table D3 and Figure D8.

Table D3 - Example rotor blade investigation event tree disposition status report table

<u>Event Tree Section</u>	<u>Total # Root Causes</u>	<u># Root Causes with Activity</u>	<u># Root Causes No Activity</u>	<u># Root Causes Closed</u>
1.1 - Lower Than Predicted Material Capability	12	8	2	2
1.2 - Higher Than Predicted Vibratory Stresses	24	12	2	10
1.3 - Higher Than Predicted Steady Stresses	17	12	1	4
Other - LCF and HCF/LCF Interaction	2	0	0	2
TOTALS	55	32	5	18

ROTOR BLADE EVENT TREE

Status as of 3/4/94

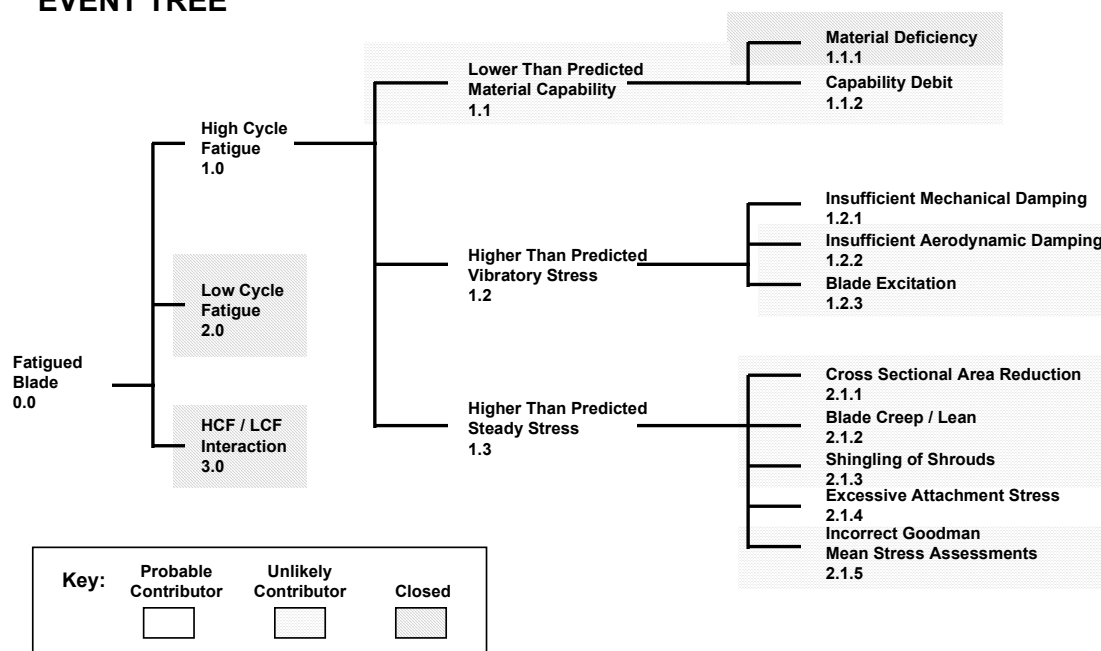


Figure D8 - Example status report event tree

As the investigation progresses, all information gathered from the action items should be entered into the disposition chart. As an action item is completed and the resulting supporting or refuting evidence is entered into the disposition chart, the root cause should be reassessed for its potential for contribution to the failure. Another action item may be assigned to gather more information, and/or its priority may be reassessed. If there is sufficient evidence that the root cause did not contribute to the failure, the root cause may be presented for closure.

Each root cause should be evaluated for its potential to contribute to the failure based on existing evidence and technical expertise. While this may not be feasible, it should be ensured that, as a minimum, every root cause is evaluated for its potential to contribute to the failure based on existing evidence and technical expertise. Often, as data is being gathered to substantiate the contribution of root causes, other problems may become apparent which did not contribute to the failure, but are considered significant enough to consider for corrective action. While these are not considered part of the failure investigation, they are a beneficial side-effect of the thoroughness of the root cause analysis, and can be a significant source of process or product improvement ideas.

Another consideration when evaluating root causes for their potential contribution to the failure is their effect when combined with other potential root causes. While a single root cause by itself may not credibly cause the failure, two or more occurring in conjunction may be sufficient to cause the failure. The technical expertise of the investigation team members should allow for awareness of potential interactions of root causes. The evidence gathered on each root cause should generate discussion of the potential for two or more root causes occurring together. In the rotor blade event tree example, the properties illustrated on the Goodman diagram make it entirely possible that neither moderately high vibratory stress nor moderately high steady stress alone will cause the blade fracture, yet when both are moderately high, they exceed the material capability curve, and the blade fractures. This is shown in Figure D9.

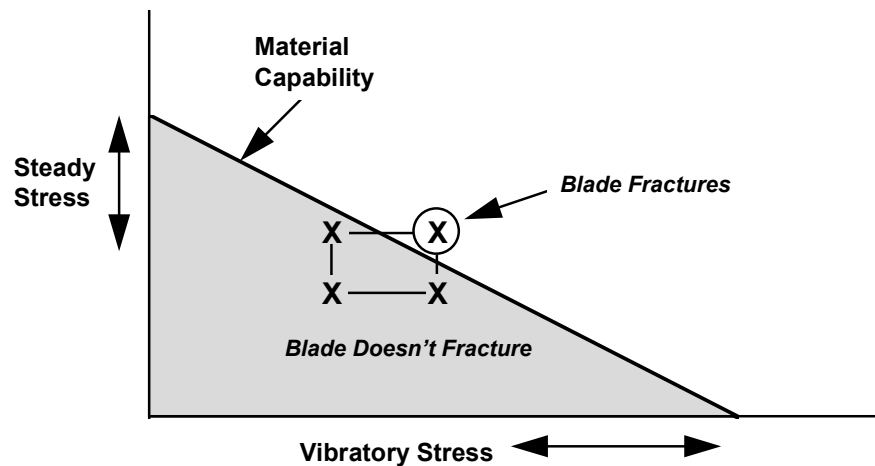


Figure D9 - Goodman diagram showing interaction of root causes

D.2.5 Dispositioning Root Causes

Closure of a root cause as a non-contributor to the failure requires agreement from all investigation team members that sufficient refuting evidence exists for the root cause, and that it is not feasible or practical to gather more evidence pertaining to the contribution of the root cause. Closure for some root causes is straightforward, while closure for others may involve some conjecture due to the unavailability of physical evidence or limited resources available to the investigation team.

Closure of events may occur at either the root cause level or at the branch level. When closing events at the root cause level, the supporting and refuting evidence that directly addresses the root cause, as it applies to its branch, is considered. If all of the root causes in a branch of the event tree are closed, then the entire branch is closed, as demonstrated in Figure D10. Thus, if root causes 1.1 and 1.2 are each closed based on the refuting evidence for each, then the entire branch 1.0 is closed. Conversely, if enough refuting evidence exists for an event at the branch level, the entire branch may be closed, along with all other events and root causes which fall within that branch. This is illustrated with branch 3.0 in Figure D10, where sufficient refuting evidence was gathered for event 3.0 to allow it to be closed. When event 3.0 was closed, all events and root causes under it, including 3.1, 3.2, 3.1.1, 3.1.2, and 3.1.3, were closed by default.

The process of dispositioning events for closure continues until all evidence has been gathered and there is team consensus that no more events can be considered as non-contributors to the failure. The remaining events and root causes on the event tree are the most likely causes that contributed to the failure.

D.2.6 Results

D.2.6.1 Analysis of the Results

When the investigation team agrees that no more events on the tree are candidates for closure, there will be one or more root causes, which remain as the most likely contributors to the failure. The investigation team should consider whether the remaining root causes interacted to cause the failure, or whether they are simply the few most probable contributors to the failure, where limited supporting evidence makes it impossible to determine, which was the true cause. In the former case, corrective action addressed to at least one (the most influential) of the remaining root causes may prevent the failure from occurring by disabling the other root causes or reducing their detrimental effect. In the latter case, corrective action may need to be addressed to all remaining root causes.

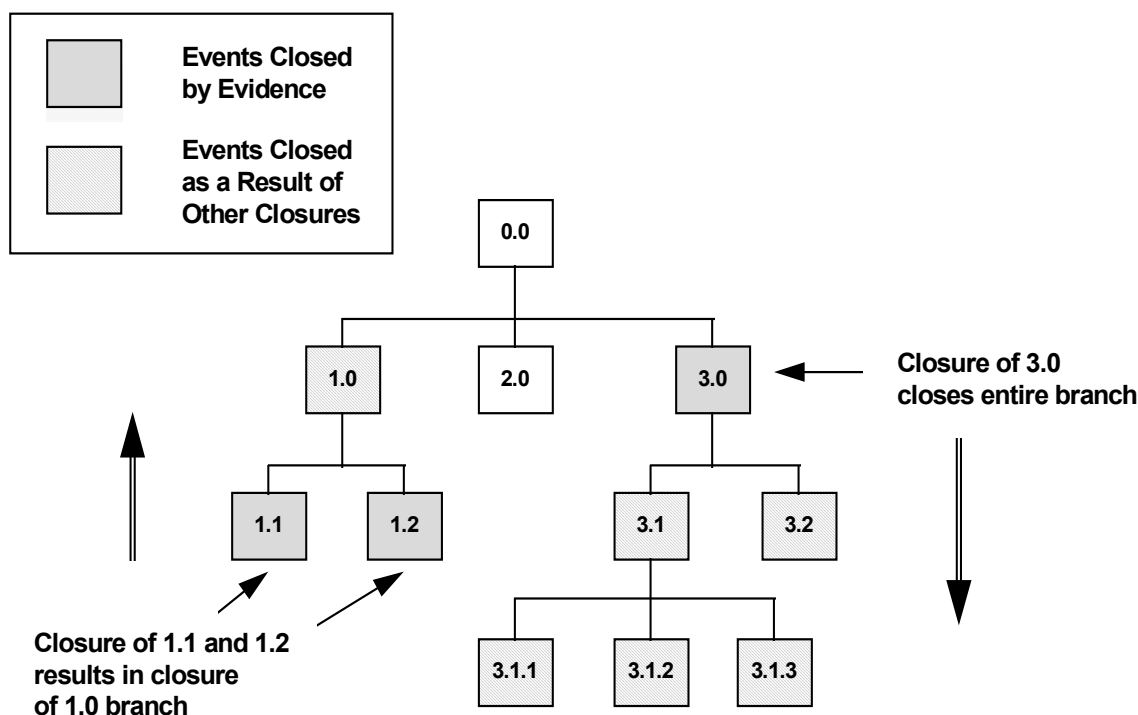


Figure D10 - Closure of events

In a hardware failure investigation, the remaining root causes on the event tree may be considered the "hardware root causes," in that they are hardware or system operation anomalies which caused the system failure. These hardware root causes may be pursued further to find the "true" root causes of the system failure, which are usually process or procedural issues. For example, if the hardware root cause was determined to be a misassembly, potential procedural root causes could include such things as unclear assembly instructions, inadequate training, lack of misassembly proof features, or insufficient quality checks. The pursuit of these procedural root causes of the failure after the hardware root cause has been determined will aid in the identification of areas to be targeted for process improvement and recurrence control.

D.2.7 Documentation

When the failure investigation is complete, the three root cause analysis tools will provide the investigation team with a complete record of all potential scenarios considered in the investigation, all evidence gathered to both support and refute each of the potential scenarios, a complete record of all actions performed under the investigation, and a listing of the top contributing root causes of the failure.

The event tree provided a visual depiction of all plausible causes, which were considered for their contribution to the failure. The mechanical principles on which the failure was based were included in the structure of the event tree, where possible, and enough detail was provided in the levels of events such that the path each root cause traced to the top event showed how each event could cause the failure. The status of the investigation, including the final remaining root causes, was depicted on the event tree.

The root cause disposition sheets with the action item list provided full traceability of all data collected and work performed to reach closure for the non-probable root causes, as well as supporting evidence for the most likely root causes in the event tree. This includes not only a description of what the resulting information was, but also the action performed to get it, the responsible individual, and the date it was performed.

The full package of the event tree, disposition sheets, and action item list may be kept in an investigation library. If the event tree has been constructed with enough detail by including all plausible causes, it will provide a starting point for event trees to be used for similar investigations. Since the event tree structure is based on the mechanical principles of the failure, it will show a great deal of commonality with event trees for other investigations of similar failure modes. The disposition charts and action item lists can provide guidance for the types of data needed to establish closure of events, as well as a list of knowledgeable individuals with experience in failure investigation.

D.3 CONCLUSIONS

The root cause analysis technique of conducting a failure investigation has several advantages:

- a. It provides full documentation of all evidence gathered and actions performed as part of the investigation.
- b. It provides rationale for closure of non-contributing causes to the failure.
- c. It has the potential for identifying more than one contributor to the failure.
- d. It conducts a thorough investigation of all plausible causes of a failure.
- e. It has the potential for identifying other product or process problems, both related and unrelated to the failure.
- f. It provides the customer with visibility into the method and progress of the investigation.

There are several secondary effects of conducting a root cause analysis. The most significant is that the thoroughness of the investigation greatly increases the chance that the true root causes of the failure have been identified and can be addressed with appropriate corrective action. Also, because every aspect of the system as it exists in this failure mechanism has been examined, the investigation team will gain a better understanding of the system. This may lead to identification of areas for process improvement, and/or this gained knowledge can be incorporated into related designs. Finally, management and the customer will have greater confidence that their resources have been appropriately used for an effective failure investigation.

D.4 REFERENCES

With the power of the Internet, a person can find many resources that discuss Root Cause Analysis. Some recommendations would be resources that include "Ishikawa Diagrams," "Fishbone Diagrams," and "Event Trees." Professor Kaoru Ishikawa created *Cause and Effect Analysis* in the 1960s. The technique uses a diagram-based approach for thinking through all of the possible causes of a problem.

APPENDIX E - WEIBULL ANALYSIS

NOTE: The basic ARP5150 document contains information that places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

E.1 SCOPE

This appendix describes the Weibull distribution and its application to reliability and safety assessment. The material should be considered an introduction to the subject, as only the basic principles and procedures are covered. This appendix is not meant to be a definitive procedural guide to the theory of Weibull analysis and all its methodological variants. References are listed at the end of the appendix for those desiring a more advanced treatment.

E.2 DESCRIPTION

Weibull analysis is used in the aviation industry to assess the reliability of airplane systems or components. Its primary distinguishing feature is that it quantifies reliability (or risk of failure) as a function of the age of the product. This makes it an ideal tool for such things as predicting warranty costs and establishing cost-effective maintenance schedules. Weibull analysis can also be used to help understand and quantify a field-revealed potential safety problem. For example, Weibull analysis can help assess whether a field recall is needed and, if so, what the appropriate recall schedule should be.

The results of a Weibull analysis are often presented graphically on specially-designed graphs where the x-axis is in logarithm scale and the y-axis is in logarithm-logarithm scale. The x-axis scale is item age, such as hours or cycles of service. The y-axis scale is cumulative percent failed. On such a graph, a two-parameter Weibull plots as a straight line. Figure E1 is an example of a Weibull distribution graph.

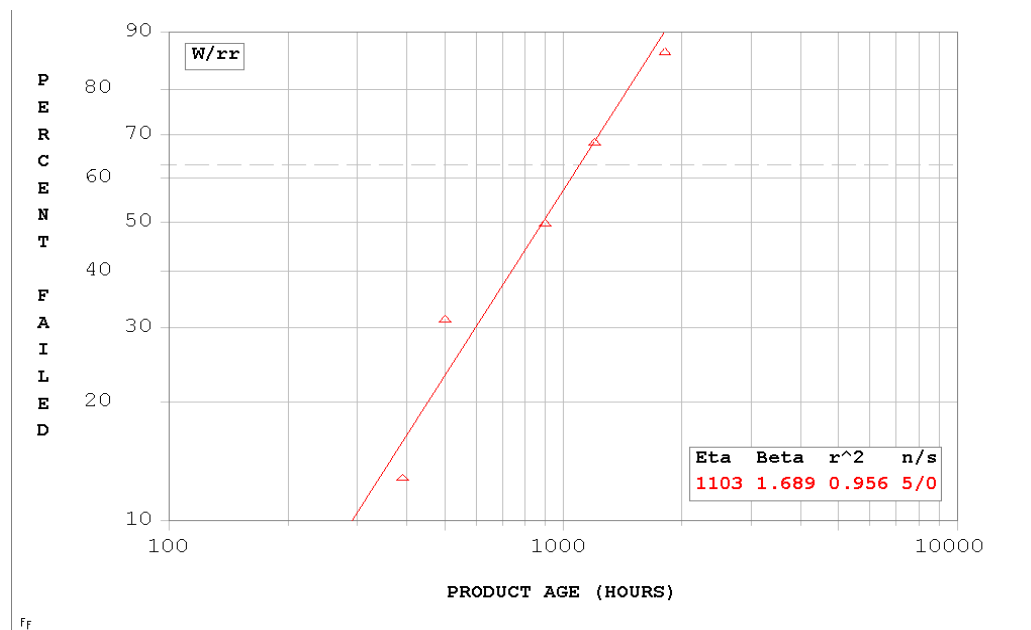


Figure E1 - Sample Weibull plot

The results of a Weibull analysis can also be presented in equation form, shown in Equation E1.

$$F(t) = 1 - e^{-(t/\eta)^\beta} \quad (\text{Eq. E1})$$

where:

$F(t)$ = Cumulative Distribution Function (CDF), which gives probability of failure by age t

η = Weibull characteristic life

β = Weibull slope

t = service life (or time of concern)

The parameters of the Weibull distribution are the characteristic life, eta (η), and the slope, beta (β). The characteristic life is the scale parameter, and is somewhat analogous to the mean of a Normal distribution. The slope is the shape parameter, and is somewhat analogous to the standard deviation of a Normal distribution. This analogy to the normal distribution can be helpful because it reinforces the statistical nature of Weibull analysis, and because it relates its ability to quantify both an expected value and the variability about that value. However, as will be discussed in later sections, the Weibull distribution has features quite distinct from the Normal distribution. Additionally, note that “-3 sigma” has no meaning against a Weibull distribution. A commonly-used analogous value in the Weibull is the B0.1 life, the age by which 0.1% of the population has failed.

Data that are Normally or Log-Normally distributed can be well-estimated by a Weibull distribution. The Weibull also collapses to the Exponential distribution when the slope = 1.0. This ability to model data from different underlying distributions makes Weibull a good choice for the initial analysis of data when the underlying distribution is unknown. Another property of Weibull distribution that makes it highly versatile for reliability applications is that it can model all portions of the so-called reliability “bathtub curve”; i.e., it can model decreasing (infant mortality), constant (random) or increasing (wearout) failure rate characteristics.

It is often more convenient to write the Weibull equation in terms of probability of success instead of probability of failure. The probability of success, or the reliability, is simply 1 minus the probability of failure. Written in equation form,

$$R(t) = 1 - F(t)$$

$$R(t) = e^{-(t/\eta)^\beta} \quad (\text{Eq. E2})$$

where:

$R(t)$ = probability of success to age t

= reliability at age t

E.3 APPLICATIONS

This section describes a few of the many applications of Weibull analysis.

E.3.1 Assess the Probability of Reaching a Pre-established Life Goal

A Weibull plot or the Weibull equation can be used directly to assess the probability of a product reaching a pre-established life goal. For example, suppose a product's reliability can be modeled with a Weibull distribution with a characteristic life of 15000 hours and a slope of 1.5. If the product has a warranty period of 8000 hours, the probability of the product failing within the warranty period can be calculated directly using Equation E1.

$$F(t) = 1 - e^{-(t/\eta)^\beta}$$

For the example, $\eta = 15000$, $\beta = 1.5$, and $t = 8000$. Inserting these values into the above equation, we obtain:

$$F(8000) = 1 - e^{-(8000/15000)^{1.5}} = 0.3226$$

It is concluded then that 32.26% of the products will fail within the 8000-hour warranty period. Or, from a positive viewpoint, 67.74% (i.e., 100% - 32.26%) of the products will successfully reach the end of the 8000-hour warranty period. Note that the four decimal places are used to illustrate the math rather than representing the expected accuracy of the prediction.

E.3.2 Assess the Service Life Corresponding to a Specific Risk Level

The Weibull equation, Equation E1, can be rearranged to solve for t , the service life.

$$F(t) = 1 - e^{-(t/\eta)^\beta}$$

$$e^{-(t/\eta)^\beta} = 1 - F(t)$$

$$-(t/\eta)^\beta = \ln(1 - F(t))$$

$$(t/\eta)^\beta = -\ln(1 - F(t))$$

$$t/\eta = [-\ln(1 - F(t))]^{1/\beta}$$

$$t = \eta [-\ln(1 - F(t))]^{1/\beta} \quad (\text{Eq. E3})$$

To illustrate a simple application of Equation E2, suppose a product's reliability can be modeled as a Weibull distribution with a characteristic life = 5000 hours and a slope of 1.9. At what age (i.e., service life) will 50% of the products have succumbed to failure?

For the example, $\eta = 5000$, $\beta = 1.9$, and $F(t) = 0.5$. Inserting these values into the above equation, we obtain:

$$t = \eta [-\ln(1 - F(t))]^{1/\beta}$$

$$t = 5000 [-\ln(1 - 0.5)]^{1/1.9}$$

$$t = 4123 \text{ hours}$$

From this calculation, it can be concluded that 50% of the product population will fail prior to 4123 hours, and 50% will survive past that time.

E.3.3 Identify "Aging" Effect

One of the most useful features of a Weibull analysis is that the "aging" characteristic of a product can be identified directly. Based on the value of the Weibull slope, it can be directly inferred whether the product's risk of failure increases with age, is constant with age, or decreases with age. This is further explained in the Table E1.

Table E1 - Beta (slope) versus aging characteristics

$\beta > 1$	Risk of failure increases with age. Wear-out, fatigue.
$\beta < 1$	Risk of failure decreases with age. Infant mortality, burn-in.
$\beta \sim 1$	Risk of failure constant with age. Random failures. Exponential distribution.

Identifying the aging characteristic of a product can be extremely useful when selecting a maintenance plan or recall schedule. For example, if the slope is approximately equal to 1, it can be inferred that it is unnecessary to establish a fixed component replacement age or schedule unless an improved part is available for replacement. The risk of failure remains constant (independent of time), so the new replacement part will have exactly the same risk of failure as the part being replaced. If the slope is less than 1, new parts tend to fail early (also called infant mortality) and the ones that survive are more reliable than new parts. In this situation, parts clear themselves from the suspect population as they age, which may or may not represent adequate risk control. On the other hand, if the slope is greater than 1, newer parts are more reliable than older ones, and there will be a benefit to replacing older parts with new ones on a regular schedule. (Of course, the cost benefit depends on the magnitude of the reliability improvement of new parts over old ones, and the cost of the parts, cost of failure of the parts and labor needed to effect the replacements.) Examples of infant mortality problems are manufacturing defects, mis-assemblies or maintenance errors.

E.3.3.1 Illustration that Slope > 1 Indicates that Reliability Degrades with Age

The following paragraphs illustrate how a Weibull slope greater than 1 is a direct indication of an increasing risk of failure.

Suppose that a component's probability of failure can be modeled with a Weibull distribution with a characteristic life of 2000 hours and a slope of 3.0. The calculations below will compare the component's probability of failure for the interval 0 to 500 hours to the probability of failure during the equal length service period of 500 hours to 1000 hours. From the Weibull equation (Equation E1), the probability of failure is given as

$$F(t) = 1 - e^{-(t/\eta)^\beta}$$

For later use, we calculate $F(t)$ for $t = 500$ and for $t = 1000$ hours.

$$F(500) = 1 - e^{-(500/2000)^{3.00}} = 0.016$$

$$F(1000) = 1 - e^{-(1000/2000)^{3.0}} = 0.118$$

The $F(t)$ values represent cumulative probabilities. The probability of an individual unit failing from time zero to 500 hours is 0.016. The probability of an individual unit failing from time zero to 1000 hours is 0.118. Of specific interest, however, is the probability of the component failing in the additional period from $t_1 = 500$ to $t_2 = 1000$ hours given that it has already survived to 500 hours. This can be calculated by subtracting the cumulative probability of failure to t_1 [$F(500)$, in this example] from the cumulative probability of failure to t_2 [$F(1000)$] and dividing by the probability that the component survived to t_1 hours, $[1 - F(500)]$. Thus, the general form of the calculation is:

$$F(t_2|t_1) = [F(t_2) - F(t_1)] / [1 - F(t_1)] \quad (\text{Eq. E4})$$

In our example, we wish to calculate the probability the "Component fails by 1000 hours (t_2)" given that the "Component Survived to 500 hours (t_1)."

$$= [F(1000) - F(500)] / [1 - F(500)] = (0.118 - 0.016) / (1 - 0.016) = 0.104$$

So the comparison can now be made between the probability of a new component failing in the first 500 hours, and a 500-hour component failing within the next 500 hours. For the new component, the probability of failure for 500 hours is $F(t=500)$, or 0.016. For the 500-hour component, the probability of failing after an additional 500 hours, i.e., to 1000 hours, is 0.104. It can be concluded, therefore, that the older component is less reliable than the new component. This is a characteristic of all Weibull distributions with a slope greater than 1.

Through the use of Equation E4, we can calculate the risk of failure of components that have already survived to a known time t .

E.3.3.2 Illustration that Slope ~1 Indicates that Reliability is Constant with Age

As further illustration of the ability of the slope value to characterize a component's "aging" effect, consider an example where the slope is exactly equal to 1. Recall that, for this case, an older component has an equal reliability to a new component. If the characteristic life is 1000 hours, and the slope is 1, we can use Equation E2 to write:

$$F(500) = 1 - e^{-(500/1000)^{1.0}} = 0.393$$

$$F(1000) = 1 - e^{-(1000/1000)^{1.0}} = 0.632$$

The probability for this component failing at 1000 hours given the component survived to 500 hours is calculated using conditional probabilities as described earlier.

$$\begin{aligned} F(\text{from 500 to 1000}) &= (F(1000) - F(500)) / (1 - F(500)) \\ &= (0.632 - 0.393) / (1 - 0.393) \\ &= 0.393 \end{aligned}$$

So, it can be concluded that a new part has a 0.393 probability of failing at 500 hours, AND a 500 hour part has a 0.393 probability of failing at 1000 hours given the part survived to 500 hours. This illustrates that, when the Weibull slope is equal to 1, the reliability is constant with age.

For constant failure rate issues (exponential distribution), it is more common to express the CDF as:

$$F(t) = 1 - e^{-(\lambda t)}$$

Where λ is the failure rate and equals $1/\eta$, where η is the mean time to failure (MTTF).

If λt is small, an approximation to $F(t) = 1 - e^{-(\lambda t)}$ is $F(t) \sim \lambda t$.

E.3.3.3 Illustration that Slope < 1 Indicates that Reliability is Improving with Age

If the slope in a population is less than 1, caution must be exercised when making failure forecasts with that slope and the corresponding characteristic life. This is because the data being analyzed may contain multiple failure modes, such as the infant mortality parts could be a batch along with a larger population that is free from the infant mortality problem. By definition 63% of the population is forecast to fail at the characteristic life, and for a mixed population that includes a small infant mortality batch, that forecast can have extreme error. Performing a Bi-Weibull, if possible, can address this problem (see Section E.7 on advanced topics).

If the infant mortality batch (or batches) is analyzed in isolation, the slope will typically be 1 or greater, showing that the batch is characterized by either a constant failure rate with a very short MTTF or an accelerated wear-out distribution (small characteristic life). It is when the batch is combined with a larger population without the infant mortality defect that the slope of less than one would typically result.

Infant mortality situations will leave limited time to mitigate risk. If infant mortality is known or suspected, and the resultant event is of a serious nature, aggressive corrective action may be required. The keys to managing an infant mortality issue are to find a way to identify the bad batch and to determine an age at which parts can be declared to not have the infant mortality defect (they would have failed by that age if they had the defect).

Relying on seeing a slope of less than 1 is not an infallible indicator of an infant mortality issue. A population with multiple failure modes ("dirty data"), including infant mortality, can mask the infant mortality failure; i.e., the slope of the population can be ≥ 1 and the population can still have units with an infant mortality issue.

E.3.3.4 Assess Impact of Extended Warranty Coverage

The results of a Weibull analysis can be used to assess the impact of extending the warranty period of a product. To illustrate, suppose that a turbine engine's reliability can be modeled as a Weibull distribution with characteristic life 10000 hours and slope 2.0. The current warranty period is 5000 hours, and it is proposed to extend this warranty period to 6000 hours. From the Weibull equation (Equation E1), the probability of failure is given as:

$$F(t) = 1 - e^{-(t/\eta)^\beta}$$

For later use, we calculate $F(t)$ for $t = 5000$ and for $t = 6000$ hours.

$$F(5000) = 1 - e^{-(5000/10000)^{2.0}} = 0.221$$

$$F(6000) = 1 - e^{-(6000/10000)^{2.0}} = 0.302$$

The probability for this turbine engine failing by 6000 hours given it survived to 5000 hours is calculated using conditional probabilities as described earlier (see E.3.3.1).

$$\begin{aligned} F(\text{from } 5000 \text{ to } 6000) &= [F(6000) - F(5000)] / [1 - F(5000)] \\ &= (0.302 - 0.221) / (1 - 0.221) \\ &= 0.104 \end{aligned}$$

Therefore, the probability of failing within the current warranty period is:

$$F(0 \text{ to } 5000) = F(5000) = 0.221$$

And the probability of failing within the proposed warranty period extension is:

$$F(5000 \text{ to } 6000) = 0.104$$

A warranty cost factor can be calculated as:

$$\text{Warranty Cost Factor} = (B + A) / B \quad (\text{Eq. E5})$$

where:

B = baseline failure probability (with current warranty)

A = additional failure probability (during extended warranty period)

For this example,

$$\text{Warranty Cost Factor} = (0.221 + 0.104) / 0.221 = 1.47$$

It can be concluded that warranty costs will increase by approximately 47% if the warranty period is extended from 5000 to 6000 hours.

E.3.3.5 Assess Impact of Extending a Scheduled Maintenance Period

The results of a Weibull analysis can also be used to judge the impact of extending a scheduled maintenance period. For example, suppose that a gas turbine engine is currently maintained with a scheduled 1500 hour time-between-overhaul (TBO). It is proposed that the TBO period be extended to 1750 hours.

For a fair comparison, the two alternatives can be compared for a baseline 1750 hours of service. With the current 1500 hour TBO, this means that an engine will first complete 1500 hours of service, then be overhauled and put back into service for an additional 250 hours. This means, in effect, that the service period from 1500 to 1750 hours is currently operated with a “new” (i.e., overhauled) engine. With the proposed 1750 hour TBO, the engine will remain in service for the entire 1750-hour interval. This means, in effect, that the service period from 1500 hours to 1750 hours will be operated with a “used” engine, i.e., one that already has 1500 hours of service.

For this example, suppose the turbine engine’s reliability can be modeled as a Weibull distribution with a characteristic life of 3000 hours and a slope of 1.2. From the Weibull equation (Equation E1), the probability of failure is given as:

$$F(t) = 1 - e^{-(t/\eta)^\beta}$$

For later use, we calculate $F(t)$ for $t = 250$, $t = 1500$, and for $t = 1750$ hours.

$$F(250) = 1 - e^{-(250/3000)^{1.2}} = 0.049$$

$$F(1500) = 1 - e^{-(1500/3000)^{1.2}} = 0.353$$

$$F(1750) = 1 - e^{-(1750/3000)^{1.2}} = 0.408$$

With the current 1500 hour TBO period, an engine must complete two service periods in order to complete 1750 hours (the baseline comparison). First, the engine must operate from $t = 0$ to $t = 1500$ hours. Next, the engine must operate from $t = 0$ to $t = 250$ hours. The probability of failure given operating in these two service intervals is shown below:

$$F(0 \text{ to } 1500 \text{ OR } 0 \text{ to } 250) = F(1500) + F(250) - [F(1500) \times F(250)]$$

$$= 0.353 + 0.049 - (0.353 \times 0.049) = 0.385$$

With the proposed 1750 hour TBO, an engine completes the 1750-hour baseline period with one service interval. The probability for failure in this interval is given above as:

$$F(0 \text{ to } 1750) = 0.408$$

A "Risk Factor for TBO Extension" can be calculated as the ratio of failure probabilities, i.e., the probability of failure for the proposed TBO period divided by the probability of failure with the current TBO period.

$$\text{Risk Factor} = F(0 \text{ to } 1750) / [F(1500) \text{ or } F(250)]$$

$$= 0.408/0.385 = 1.060$$

It can be concluded that the proposed TBO extension would increase the field failure rate by approximately 6%.

E.4 ANALYTICAL PROCEDURE

Excellent commercial software packages are available which make the "mathematics" of Weibull analysis quite simple. However, there is a potential downside to having this user-friendly software available, namely that Weibull analysis can become viewed as "using the software" instead of analyzing the product. Like many analytical tasks, Weibull analysis depends heavily on an individual's knowledge and judgment in the area. A key element of this knowledge and judgment involves understanding the underlying mathematics that the software so conveniently takes over. The discussion that follows describes how to manually perform the calculations for a Weibull analysis.

E.4.1 All Items Operated to Failure

The simplest data set to analyze is when a group of items are operated to failure. This, of course, is not likely to occur with a fielded product but is quite common with in-house testing. The steps involved in analyzing this data, using the median rank method are as follows:

1. Arrange the failure times in ascending order.
2. Use a median rank table to assign a median rank value (i.e., probability) to each failure time.
3. Plot each data point on Weibull graph paper.
4. Graphically draw a line to best fit the plotted data points.
5. Read the characteristic life, η , from the graph. It is the intersection of the plotted line with the horizontal dashed line located at $F(t) = 63.2\%$. This horizontal dashed line is a permanent part of the grid on any Weibull graph paper.

6. Read any other $(t, F(t))$ value from the plotted line, giving $(t_1, F(t_1))$.
7. Calculate the slope from Equation E6.

$$\beta = (\ln(-\ln(1-F(t_1)))) / \ln(t_1 / \eta) \quad (\text{Eq. E6})$$

where η is known from step 5, and t_1 and $F(t_1)$ are known from step 6.

NOTE: Equation E6 is simply an algebraic rearrangement of the Weibull equation, Equation E1.

E.4.1.1 Example Number One

To illustrate the steps listed above, consider a group of five turbine engines, which accumulated the following service times before failing.

Table E2 - Example no. 1 engine service times

<u>Operating Hours</u>	<u>Status</u>
500	Failed
390	Failed
1810	Failed
900	Failed
1200	Failed

Step 1: Arrange the failure times in ascending order.

Sorted Table E2 - Example no. 1 engine service times

<u>Order Number</u>	<u>Failure Time</u>
1	390
2	500
3	900
4	1200
5	1810

Step 2: Assign a median rank value to each failure time.

A table of median ranks can be found in most statistics or reliability textbooks. Table E3 provides a median rank table covering sample sizes up to 10. For this example, the sample size is 5 and the median ranks can be found in the corresponding column of the median rank table. The resulting median results for the example are tabulated in Table E4.

Table E3 - Example no. 1 median rank results

Order Number	Failure Time	Median Rank
1	390	0.1294
2	500	0.3147
3	900	0.5000
4	1200	0.6853
5	1810	0.8706

Table E4 - Table of median ranks

Order Number	Sample size n									
	1	2	3	4	5	6	7	8	9	10
1	0.5000	0.2929	0.2063	0.1591	0.1294	0.1091	0.0943	0.0830	0.0741	0.0670
2		0.7071	0.5000	0.3864	0.3147	0.2655	0.2295	0.2021	0.1806	0.1632
3			0.7937	0.6136	0.5000	0.4218	0.3648	0.3213	0.2871	0.2594
4				0.8409	0.6853	0.5782	0.5000	0.4404	0.3935	0.3557
5					0.8706	0.7345	0.6352	0.5596	0.5000	0.4519
6						0.8909	0.7705	0.6787	0.6065	0.5481
7							0.9057	0.7979	0.7129	0.6443
8								0.9170	0.8194	0.7406
9									0.9259	0.8368
10										0.9330

Steps 3, 4, and 5: Plot each data point on Weibull graph paper. Graphically draw a line to best fit the plotted points. Read the characteristic life where the plotted line crosses the horizontal dashed line.

Figure E2 shows the results of Steps 3, 4, and 5. As shown, the characteristic life can be graphically estimated to be 1150 hours.

Step 6: Read any other (t, F(t)) value from the plotted line, giving (t₁, F(t₁)).

As shown in Figure E2, the plotted line crosses t = 90 hours at F(t) = 2.0%. Thus (90, 0.020) can be used as values for (t₁, F(t₁)).

Step 7: Calculate the slope from the Equation E6:

$$\beta = (\ln(-\ln(1 - F(t_1)))) / \ln(t_1/\eta)$$

Inserting the applicable values for F(t₁), t₁, and η , the slope can be calculated as:

$$\beta = (\ln(-\ln(1 - 0.020))) / \ln(90/1150) = 1.53$$

Thus, based on this analysis, the engine can be modeled with a Weibull Distribution with a characteristic life of 1150 hours and a slope of 1.53.

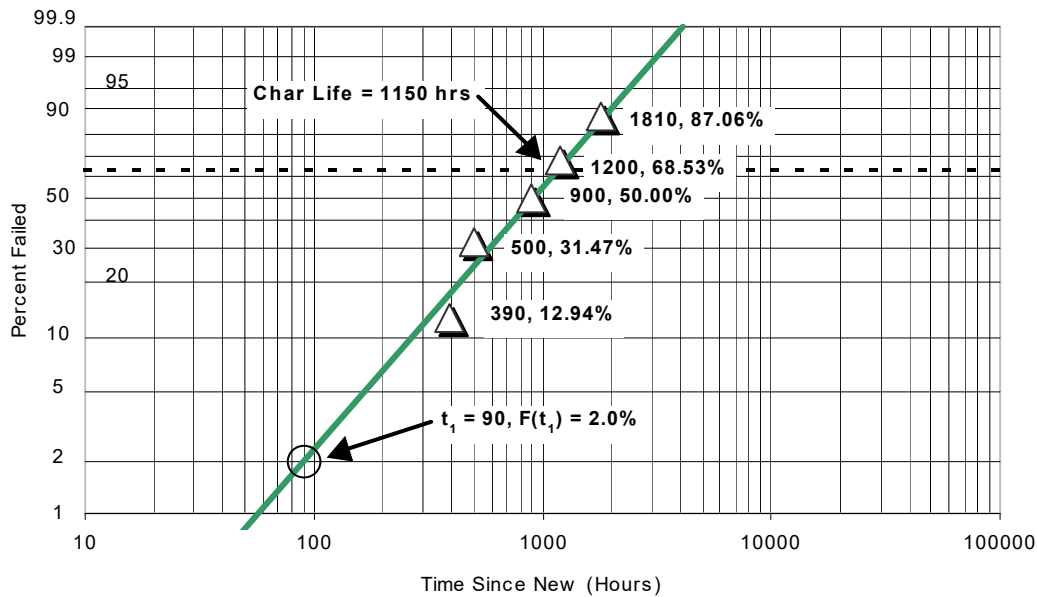


Figure E2 - Plot of example no. 1 Weibull probability

E.4.2 Data Includes Non-Failed Items

In most situations where a Weibull analysis is needed, the data includes non-failed items as well as failures. These non-failed items are sometimes called suspensions or censors. They represent items which have completed a period of operation without experiencing a failure, or which are still in active operation. A typical set of data may include the operational times on several hundred units, with perhaps only five to ten of them having failed. An accurate analysis must give appropriate credit for the successful operation of the non-failed units.

E.4.2.1 Example Number Two

As another example, consider a group of five turbine engines that have accumulated the service times shown in the Table E5. Four of the engines suffered failures, but one engine is still operating.

Table E5 - Example of no. 2 engine service times

<u>Serial Number</u>	<u>Operating Hours</u>	<u>Status</u>
17	390	Failed
9	500	Still Running
38	900	Failed
14	1200	Failed
3	1810	Failed

Notice that the operating times have been listed in ascending order. In the previous example, we assigned Order Numbers in sequence from earliest failure to highest time failure. In this case, Engine Number 9 has not yet failed. Even though this engine has the second lowest operating time, it should not be assigned Order Number 2. This engine might very well be capable of operating past 900 hours, and thus become Order Number 3. In fact, the non-failed engine might operate past the 1200 hour engine or the 1810 hour engine, becoming Order Number 4 or 5. Similarly, Order Numbers are not known for any of the failed engines except the first one (Engine 17). Table E6 below repeats the data with the possible Order Numbers for each.

Table E6 - Example no. 2 order numbers

<u>Serial Number</u>	<u>Operating Hours</u>	<u>Status</u>	<u>Order Number</u>
17	390	Failed	1
9	500	Still Running	2, 3, 4, or 5
38	900	Failed	2 or 3
14	1200	Failed	3 or 4
3	1810	Failed	4 or 5

In order to assign median ranks and plot the data on Weibull paper, we need to assign a single Order Number to each failure point. The discussion following illustrates how this can be done.

Note that, if operation continues, the non-failed unit will fail in one of the following intervals.

1. 500 hours to 900 hours
2. 900 hours to 1200 hours
3. 1200 hours to 1810 hours
4. after 1810 hours

Since there are four possibilities, each possibility can (arbitrarily) be assigned a probability of 0.25. This is analogous to assigning 1/4 of a failure to each of the four possible intervals. The table below repeats the data listing, and assigns Order Numbers based on this logic.

Table E7 - Example no. 2 resorted order numbers

<u>Engine Serial Number</u>	<u>Operating Hours</u>	<u>Status</u>	<u>Order Number</u>
17	390	Failed	1
9	500-900	1/4 Failure	1.25
38	900	Failed	2.25
9	900-1200	1/4 Failure	2.50
14	1200	Failed	3.50
9	1200-1810	1/4 Failure	3.75
3	1810	Failed	4.75
9	>1810	1/4 Failure	5.00

Now, with calculated Order Numbers, median ranks can be assigned to each of the four failure data points. This is done by interpolating within the Median Rank Table (Table E3), using the column for a sample size of 5. The results are shown in Table E8.

Table E8 - Example no. 2 median rank results

<u>Engine Serial Number</u>	<u>Operating Hours</u>	<u>Status</u>	<u>Order Number</u>	<u>Median Rank</u>
17	390	Failed	1	0.1294
9	500	Still Running	-----	-----
38	900	Failed	2.25	0.3610
14	1200	Failed	3.50	0.5927
3	1810	Failed	4.75	0.8243

The Weibull analysis can now be completed using the same procedure described earlier.

1. Plot each of the four failure data points on Weibull graph paper.
2. Graphically draw a line to best fit the plotted data points.
3. Read the characteristic life value (where the plotted line crosses the horizontal dashed line).
4. Calculate the slope of the plotted line using Equation E6:

$$\beta = (\ln(-\ln(1 - F(t_1)))) / \ln(t_1/\eta)$$

Thus, except for assigning Order Numbers, the calculation procedure is exactly the same as described earlier in E.4.1. Figure E3 shows the calculation results for this example. (The detailed calculations are not included. It is suggested that the reader perform these calculations as an exercise, and compare the results to those shown in Figure E3.)

E.5 CAUTIONS

This section will discuss two issues that frequently arise when analyzing service data.

E.5.1 Precise Failure Definition

In order to perform an accurate Weibull analysis, it is necessary to establish a precise definition of what constitutes a "failure." Specifically, the selected failure definition must allow the following:

1. The state of every item in the population must be known; i.e., it must be apparent whether each item is a failure or a non-failure.
2. For each failure, the specific age at failure must be known or estimable.

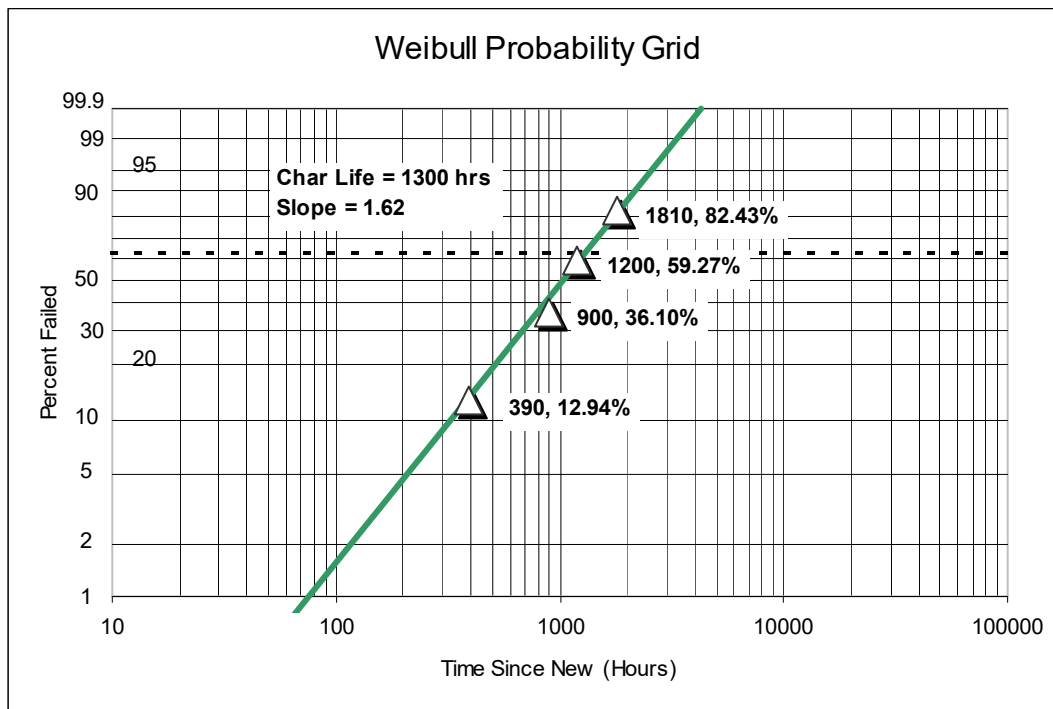


Figure E3 - Plot of example no. 2 Weibull probability

This seems easy enough, but there are often cases where the line between “failure” and “success” is blurred. A very common situation that often causes confusion is “crack” data. For example, a compressor disk might be found to have a crack when it is inspected at an engine overhaul shop. From an engine standpoint, the disk did not “fail” because it was still performing its function successfully when the engine reached its scheduled overhaul period. However, from a disk standpoint, the existence of a crack is very undesirable. The analyst must face the following questions.

1. What constitutes a failure? The choices are a) a cracked disk or b) a broken disk (which causes an engine failure).
2. When did the part fail? If a “cracked” disk constitutes failure, when did the crack occur? If a broken disk constitutes failure, when would the observed crack have propagated to failure?
3. Are there additional “failures” in the fleet? If a “cracked” disk constitutes failure, are there some non-inspected disks which might also be “cracked”? If a broken disk constitutes failure, the problem is simpler. For this case, all disks in operating engines are non-failed (since an engine cannot operate with a broken disk).

It is quite common to perform a Weibull analysis using the crack discovery times as the failure times. When this is done, the Weibull becomes a model of “time to crack discovery” rather than “time to failure (crack).” The problem is that “crack discovery” is a function of when the part was inspected. Inspection reliability is also a factor. Thus, there is additional variability in the time to crack.

When “crack” data is involved, a skilled analyst will follow one the following approaches.

1. Define failure as crack initiation. Then use fracture mechanics to estimate the crack initiation time; i.e., how many cycles prior to the inspection did the crack initiate? In addition, inspect all other components in the fleet to determine if they are cracked. (If any more cracked components are found, their crack initiation time must also be estimated).

If it is not possible to inspect all components, the only suspensions used in the Weibull should be those components known to be crack-free, and the age at which that determination was made. In other words, if a component was inspected at 4000 hours and found to be crack-free, but is now 5000 hours in age, the time at inspection (4000 hours) should be used. If the component has never been inspected, it can only be assumed to be crack-free at 0 hours. Unfortunately using only crack-free inspection results as suspensions can result in a conservative analysis, which may not be appropriate for the intended use of the analysis.

If true crack initiation time cannot be estimated via fracture mechanics (or striation counting), analysis that adjusts for crack length is often illustrative. Due to the confounding factor of discovery time - the situation that components may not be inspected until a certain age - the Weibull may over-estimate the slope (because all cracks *appear* to have initiated at the same time. By performing repetitive Weibulls for different crack sizes (for example, Weibulls with cracks of at least 0.25 inch, at least 0.5 inch, at least 0.75 inch, at least 1.0 inch) for the same data yields fewer "cracks" and more suspensions as crack size increases, and this may give a more representative slope as longer crack sizes are used. As an additional benefit, the different Weibull lines can serve as an estimate of crack propagation.

2. Define failure as component separation or obvious malfunction. Now many, if not all, uninspected parts can be counted as suspensions, as it is known whether they've failed. Use fracture mechanics to estimate how many additional cycles any cracked component could operate until complete separation. Alternatively, the cracked component could be placed on a test rig and operated until failure. When using fracture mechanics to estimate the final failure, use a load level that is likely for the failure. This load may be a fairly routine load, not a severe design load case.

Using a 3-parameter Weibull may be useful in this situation. The slope and characteristic life correspond to crack initiation (or some other small crack size, e.g., detectable crack size), and the location parameter (the third parameter in a 3-parameter Weibull) is used for the additional time to grow the crack from the defined small size to the final failure (component separation or major obvious malfunction).

3. If fracture mechanics results are not available, the relationship between the crack initiation distribution and component failure distribution can be used to derive an estimate of a crack propagation distribution. It seems reasonable to assume that the difference between the crack initiation B50 life (the age at which 50% of the parts are predicted to have a crack initiated) and the failure B50 life is a good estimate of the crack propagation B50 life. Note that the propagation slope is likely not the same as the initiation or failure slope. Iteration may be required to find a propagation distribution that, when added to the known initiation distribution, matches the known failure distribution.

E.5.2 Multiple-Mode Weibulls

The Weibull distribution has proven, empirically and analytically, to be an excellent model for many individual failure mechanisms on individual components. Its accuracy in modeling single failure modes has been widely recognized. On the other hand, a Weibull distribution may not be the optimum model for a system or product with multiple failure modes. One failure mode may be predominant early in the product's life, while a separate failure mode becomes predominant later. There may be multiple failure modes (overload versus fatigue, for example) that have different Weibull slopes. The result may be that the combined failures do not plot as a straight line on Weibull plot (see References for more information). On the other hand, they *may* plot as a straight line if many failure modes are present. This is the case for turbine engine inflight shutdowns (IFSDs), which have a wide variety of causes with different failure probabilities and thus different Weibull slopes. But, when combined together, they result in a random distribution which may quite readily be used to predict the overall rate of IFSD.

Difficult or not, there are times when an analyst needs to determine a failure distribution for a product with multiple failure modes. A preferred approach, if enough data is available, is to perform a Weibull analysis on each mode separately and then combine them mathematically to obtain the overall product distribution. But often, there are few failures on the individual modes. Or, worse, product failures are reported but details of the failure mode(s) are not. In this case, a Weibull analysis of the overall product may be the best available choice.

From a practical standpoint, a Weibull distribution is simply a mathematical equation. If the plot of a given set of data forms a straight line on a Weibull plot, it is probably reasonable to use the Weibull distribution as a model. This is true whether the data comes from a single mode or from multiple modes.

Bi-Weibull and 3-Parameter Weibull are two tools mentioned in the section titled "List of Advanced Topics." These distributions can, many times, more accurately model an overall product that has multiple failure modes, providing those failure modes can be identified and the failures correctly assigned to them. Their advantage is that they are more flexible, and can fit data that does not form a straight line on Weibull graph paper. Many Weibull software programs will perform goodness of fit tests.

E.5.3 Spline Fits

When all else fails in trying to obtain a reasonable fit to the data, it is possible to harken back to the days of French curves and hand fits, though many computer programs will fit splines of various orders (quadratic, etc.) upon command. The intent is not to force a line through each of the points, but rather to create a smoothed line through the data. Strictly speaking, this is no longer a Weibull (or lognormal, or other distributional) fit, but a best fit through the data in an attempt to characterize the general progression of failures as components age. Such a fit can help determine failure percentiles from the fitted curve.

E.5.4 Weibull Slopes with Few Failures

The calculation of a Weibull slope given a small number of failures should be treated with caution. As an example, the occurrence of two failures with low times that are almost identical will produce a Weibull slope that is very steep, indicating a strong wearout mode. However, if the non-failure population is predominantly older than the parts that have failed, an infant-mortality mode (slope < 1) may be more appropriate. In a situation as this, calculation of the slope using the Maximum Likelihood Estimation (MLE; see Section E.7) may provide a more accurate solution. This also may be an indication that multiple subpopulations exist within the total population.

Another approach is to use historical knowledge of that type of failure mechanism to estimate the range of slopes that would be characteristic (infant mortality, constant rate, wearout) of that particular failure mode. Performing a Weibest/Weibayes analysis (see Section E.7) using the range of slopes can be useful in bounding the probability of a future failure.

E.6 WEIBULL HAZARD RATE FUNCTION

As mentioned earlier, a key feature of Weibull analysis is that it evaluates how a component's risk of failure changes with age. The primary output of a Weibull analysis is the cumulative distribution function, depicting percent (of the population) expected to fail versus operating time (i.e., component age). It is often more useful to display the Weibull analysis results in terms of the hazard rate, which more directly quantifies how risk changes as the component accumulates service time.

E.6.1 Hazard Rate Equation

The hazard rate of a component life distribution is sometimes referred to as the instantaneous failure rate. That is, it represents the probability of a component failing in the short interval of time Δt from age t to $t+\Delta t$, given that it had not failed at time t . The hazard rate is not a distinct distribution, but simply another way to represent the specific life distribution. Mathematically, the hazard rate for a given age t is defined as:

$$h(t) = f(t) / (1 - F(t)) \quad (\text{Eq. E7})$$

where:

$f(t)$ = probability density function

$F(t)$ = cumulative probability function

For a Weibull distribution, where η = the characteristic life and β = Weibull slope, the hazard rate is defined by Equation E8:

$$h(t) = (\beta/\eta) (t/\eta)^{(\beta-1)} \quad (\text{Eq. E8})$$

For constant failure rates the hazard function is constant and equals λ (recall that $\lambda = 1/\eta$). In other words, the Weibull collapses to the exponential distribution for $\beta = 1$.

E.6.2 Graphical Representation of Hazard Rate

Figure E4 shows the cumulative distribution function for two Weibull distributions having the same median life (1000 hours), but significantly different risks at other ages. One distribution has a Weibull slope of 0.7, indicating infant mortality. The second distribution has a Weibull slope of 2.0, indicating a wearout condition. If the units in service for the two populations had accumulated a typical service time of 1000 hours, the observed (average) failure rate would be very similar. However, if these same populations were then continued in service for an additional 1000 hours, the observed failure rate would be quite different. In fact, the observed rate for this continued service would be quite different from the initial 1000 hours, and the two populations would be quite different from each other. Note that predictions to high-time failures for infant mortality distributions are likely not accurate (see E.3.3.3.).

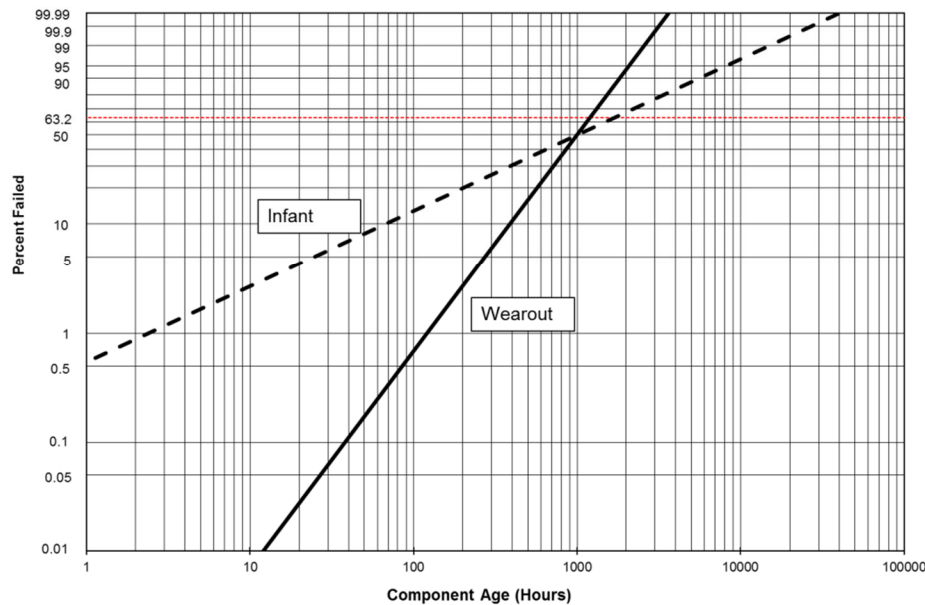


Figure E4 - Cumulative distribution for two Weibulls having the same median life

Figure E5 shows plots of the hazard rate for both the infant Weibull distribution ($\beta = 1.2$) and the wearout Weibull distribution ($\beta = 3.5$). Note that predictions to high-time failures for infant mortality distributions are likely not accurate (see E.3.3.3.).

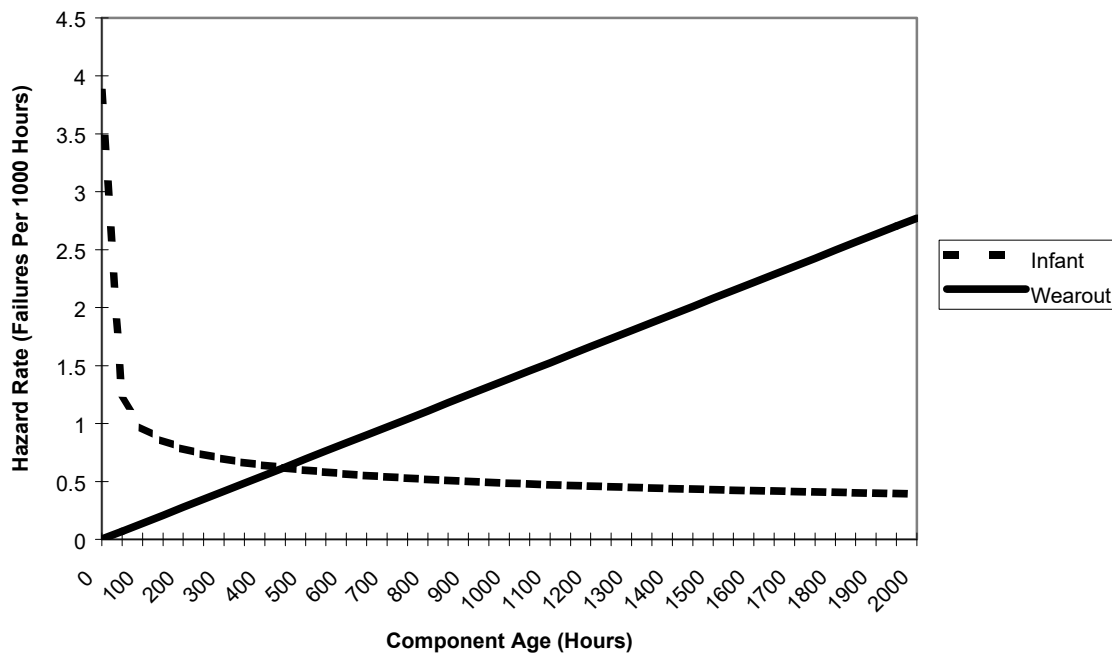


Figure E5 - Hazard rate curves for infant mortality and wearout

As the graph clearly shows, the failure risk for the infant component is high at entry into service and improves very quickly. The failure risk for the wearout component is low at entry into service, but worsens steadily as service continues. The two components have equal risks at approximately 450 hours into service.

E.6.3 Age-Focused Corrective Action Implementations

A clear application for the hazard rate distribution is to judge whether to focus on specific aged components when implementing a fleet corrective action plan. When the hazard rate indicates a strong wearout characteristic, fleet risk could be improved much more quickly by scheduling corrective action on the higher age units prior to the newer ones (or take action on newer ones once they reach some threshold age). Conversely, when the hazard rate indicates infant mortality, the fleet risk could be most quickly improved by addressing the low time units first.

E.7 LIST OF ADVANCED TOPICS

As mentioned in the Scope, the material in this appendix should be considered an introduction to the subject of Weibull analysis. Several advanced topics have not been covered. A few of these advanced topics are listed below, along with a brief description. The interested reader may consult one or more of the references provided in Section E.8 for more details.

- a. **Confidence Intervals:** A confidence intervals can be placed on the calculated Weibull characteristic life, the calculated slope, or on any life versus probability value (Bx.x). The confidence intervals provide an accounting of statistical uncertainty, which is a function of sample size and inherent variability. Confidence intervals also provide guidance as to whether the difference between two or more Weibulls is due to chance or is statistically significant. Weibulls by parameter (operator, usage, etc.) are frequently performed to investigate contributing factors.
- b. **Maximum Likelihood Estimation (MLE):** This analysis method is an alternative to the median rank method described in this Appendix. The MLE is often used in situations with few or no failures. Note that the MLE-fitted line may not go through the observed failure points in a least-squares sense like the median rank fit.
- c. **Three-Parameter Weibull Distribution:** This distribution includes a third parameter, location, in addition to the characteristic life and slope. A three-parameter Weibull distribution plots as a curved line on basic Weibull paper. Three-parameter Weibulls are used when there is a minimum time before a failure is possible. Standard two-parameter Weibull analysis can be used for estimating the three-parameter Weibull by iterating on the location parameter and subtracting it from each age value in the data and then fitting a standard Weibull until a good fit is attained.

- d. Two-Segment Weibull (Bi-Weibull; dogleg bend): This distribution is defined by two Weibull segments that intersect. Thus from $t = 0$ to $t =$ the intersection point, a distribution is defined by the first Weibull segment. For t values greater than the intersection point, another distribution is defined by the second Weibull segment. Two-segment Weibulls are indicative of multiple failure modes in the data; note that failures of both modes can be present in each segment. They can also be used for a product that begins service subject to infant mortality, but enters a wearout mode after a specific time in service.
- e. Weibayes/Weibest Analysis: This method provides the capability to estimate Weibull parameters when there have been few or no failures. The method is based on assuming the slope, or using similar historical data to estimate it. It also allows comparison of the “ideal” distribution (given the number of failures and the suspension times) to the actual. If the “ideal” Weibest is outside the selected confidence band of the actual Weibull, the suspect parts are likely a subset of the complete population (with the selected level of confidence).

When the slope (β) is assumed, the characteristic life (η) is the only parameter that needs to be calculated, as in the formula below.

$$\eta = \Sigma [(t^\beta)/r]^{(1/\beta)} \quad (\text{Eq. E9})$$

where:

r = total number of failed units and the summation is over the entire population (failures plus suspensions)

If performing a Weibayes for a three-parameter Weibull where both the slope (β) and the location parameter (γ) are assumed:

$$\eta = \Sigma [(t - \gamma)^\beta / r]^{(1/\beta)} \quad (\text{Eq. E10})$$

And the summation is only over the units with t greater than γ .

E.8 REFERENCES

- a. USAF Weibull Analysis Handbook, R. B. Abernethy, J. E. Breneman, C. H. Medlin, G. L. Reinman, AFWAS-TR-83-2079, November 1983.
- b. The New Weibull Handbook, 5th Edition, Robert B. Abernethy, December 2006.
- c. Applied Life Data Analysis, Wayne Nelson, John Wiley & Sons, 1982.
- d. Statistical Models and Methods for Lifetime Data, Jerald F. Lawless, John Wiley & Sons, 1982.
- e. Reliability in Engineering Design, K. C. Kapur, L. R. Lamberson, John Wiley & Sons, 1977.
- f. Statistical Methods for Reliability Data, William Q. Meeker and Luis A. Escobar, Wiley, 1998.

APPENDIX F - MONTE CARLO SIMULATION

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the body of the document.

F.1 INTRODUCTION

Monte Carlo simulation is a versatile method of analyzing problems that are probabilistic in nature. The analysis involves defining a mathematical model of the system being studied and operating the model repeatedly in order to observe the range of system outcomes. The model typically involves several probabilistic input parameters, where the parameter values are defined by probability distributions. The model also defines how these input parameters combine with each other and with non-probabilistic parameters to produce specific potential system outcomes.

The inputs to an aviation safety model might include the failure distributions of contributing failure modes, reliability of fault monitoring and accommodation provisions, scheduled inspections and repair intervals, effectiveness of maintenance actions, effectiveness of crew actions, flight conditions, etc. Although the output format of a Monte Carlo simulation is often tailored to the specific problem being studied, a typical output would be a prediction of the number of hazardous events for the time period being studied (e.g., the next year, five years, or until fleet retirement). Other outputs may include prediction of inspections, malfunctions or failures, and replacement components required to allow for efficient provisioning across time.

For fleet problems requiring a corrective action, the Monte Carlo method can be used to help judge the acceptability of various proposed corrective actions and implementation schedules. Corrective action input might be proposed changes to equipment design, revised inspection or maintenance schedules, constraints on flight conditions, etc. Likewise, implementation schedule changes might be modeled to judge the benefit of various accelerated schedules. The Monte Carlo output (e.g., the number of hazardous events) is then compared to that of the baseline (uncorrected) analysis to evaluate the effectiveness of the proposed corrective action(s) and implementation schedule(s).

Monte Carlo simulation is a stochastic technique, meaning that the outcome is a probabilistic function of the inputs. The simulation typically involves hundreds, thousands, or even millions of "trials" of system operation. Analyzing an event with the probability of $1.0E-9$ may require billions of trials (there are also simulation techniques that model only the tails of distributions). For each trial, a specific value for each input parameter is randomly selected from the specific probability function for that parameter. The "random" selection of each input value is accomplished through a pseudo-random number generator.

A single Monte Carlo trial is analogous to performing a test, and the analyst is responsible for running enough trials to obtain the desired confidence in the simulation results. The advantage of Monte Carlo over analytic methods such as fault tree and Markov is that more complex system behavior and probability distributions can be modeled. For those systems where fault trees and Markov are adequate, they would likely provide a quicker answer.

F.2 ELEMENTS OF A MONTE CARLO SIMULATION

Analyzing a problem with Monte Carlo simulation involves several steps as described below.

1. Define the problem to be analyzed.
2. Identify the parameters that contribute to or influence the problem.
3. Define a mathematical expression for each input parameter. Each probabilistic input parameter is defined with a probability distribution. Input parameters which are non-probabilistic (i.e., deterministic parameters) are defined with simple mathematical equations such as "Component Retirement Age = 10000 hours."
4. Define the relationship between the output event (problem) and the input parameters.
5. Define the content and format of the output desired from the simulation.

6. Develop a computer simulation program which uses the program inputs to calculate the outputs, and summarize the results in the desired format.
7. Operate the computer program, obtain the results, and communicate the results to the individuals and groups responsible for further action or decision making related to the problem.

F.3 PROBABILITY DISTRIBUTIONS

As stated earlier, each probabilistic input parameter to the Monte Carlo simulation should be described by a probability distribution or range of possible inputs. All probability distributions can be grouped into two major categories. The first category, Discrete Distributions, includes distributions where the parameter values must be constrained to specific values. The second category, Continuous Distributions, includes distributions where the parameter can take any value in a specified range.

F.3.1 Discrete Distributions

Discrete distributions are used when the parameter values must be constrained to specific values. One example would be the effectiveness of an inspection, where the possible outcomes are “defect found” or “defect missed.” Another example would be the number of flights for a specific aircraft for a particular day, where the possible outcomes are 0, 1, 2, 3, etc. For a discrete distribution, each possible parameter value must have a probability of occurrence defined, and the sum of the probability values of all possible parameter values must be equal to one.

F.3.1.1 Simple Example - Two Outcome Model

A simple, but common, example of a discrete probability distribution is a two-outcome model for the effectiveness of an inspection. For example, perhaps a specific inspection technique has been determined to be 80% effective. This means that, given that a defect exists, the inspection will detect the defect 80% of the time. Conversely, the defect will not be discovered 20% of the time. This situation is depicted in the histogram in Figure F1.

To include the influence of this “Inspection Efficiency” distribution in a Monte Carlo simulation model, simply include steps similar to those shown below. The term “Random Number” in this appendix represents a sample drawn from a uniform distribution having a range 0 to 1. F.3.2.1 describes the uniform distribution.

1. Sample a Random Number.
2. If the Random Number is less than or equal to 0.8, then assign “Defect Detected.”
3. Otherwise, assign “Defect Missed.”

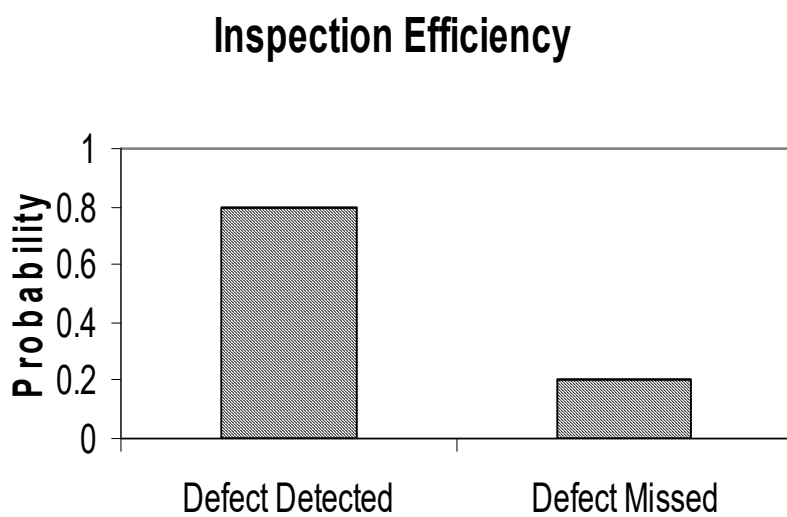


Figure F1 - Inspection effectiveness

F.3.1.2 Simple Example - Multi-Outcome Model

Another example of a parameter best modeled with a discrete distribution is the number of flights flown by an individual aircraft on a specific day. For example, historical data might determine that an aircraft from a particular airline will fly as many as six flights in a day, or as few as zero. The specific probabilities for each of the possibilities can be determined from historical data and are shown in Figure F2.

To include the “Number of Flights in a Day” as a variable in a Monte Carlo simulation model, it is first necessary to convert the probability data from Figure F2 into a cumulative probability or stacked format, as shown in Figure F3. While the stacked format has little intuitive value in describing the “Number of Flights in a Day” data, it allows the various parameter values to be modeled as unique, mutually exclusive probability slices. The “Number of Flights in a Day” can then be included in a Monte Carlo model by using mathematical steps similar to those shown below:

1. Sample a Random Number.
2. If “Random Number” is less than or equal to 0.05, then assign “Zero Flights.”
3. If “Random Number” is greater than 0.05 but less than or equal to 0.15, then assign “One Flight.”
4. If “Random Number” is greater than 0.15 but less than or equal to 0.35, then assign “Two Flights.”
5. If “Random Number” is greater than 0.35 but less than or equal to 0.65, then assign “Three Flights.”
6. If “Random Number” is greater than 0.65 but less than or equal to 0.90, then assign “Four Flights.”
7. If “Random Number” is greater than 0.90 but less than or equal to 0.95, then assign “Five Flights.”
8. Otherwise, assign “Six Flights.”

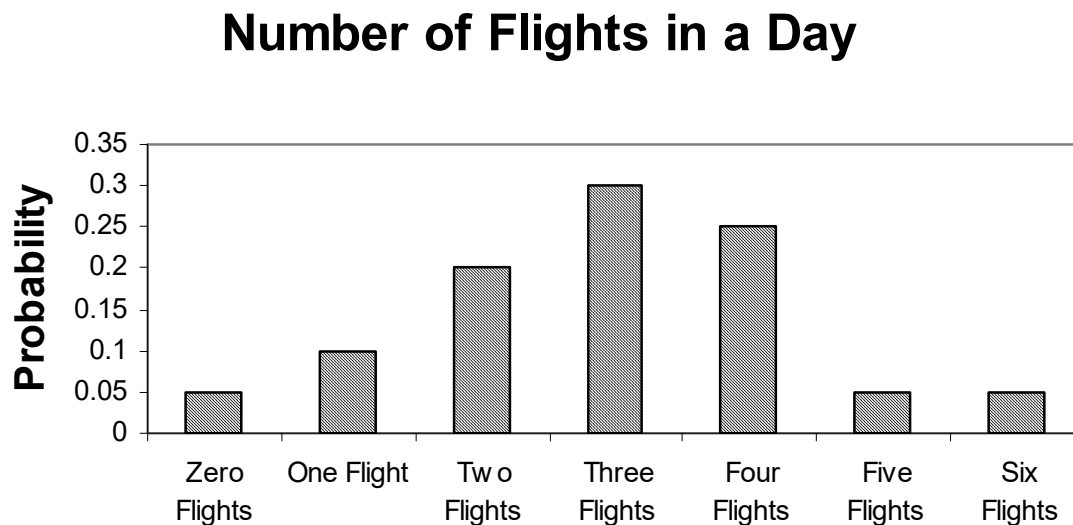


Figure F2 - Probability for flights based on historical data (distributed format)

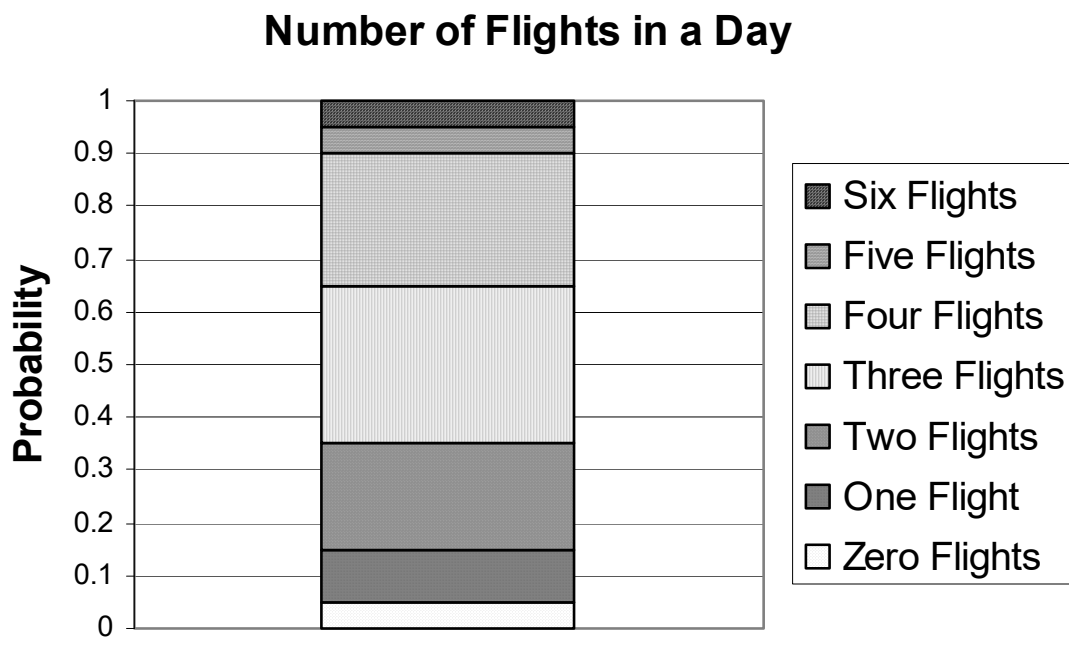


Figure F3 - Probability for flights based on historical data (stacked format)

F.3.2 Continuous Distributions

Continuous Distributions are used when the parameter being modeled can take any value in a specified range. One example would be component time to failure, where the time can be any value greater than 0. Other examples include the flight time for a specific flight, the length of a crack, the growth rate of a crack, and the diameter of a shaft.

F.3.2.1 Generating Values from Continuous Distributions

The cumulative distribution function for a continuous distribution, $F(x)$, represents the probability that a variable drawn from that distribution is less than x . $F(x)$ may be available as an equation or may be obtained from a tabulation; in which case, the sampled variable must be scaled to get it into the range of the tabulation. Samples from the distribution $F(x)$ are obtained in two steps:

1. Generate a "Random Number" b .
2. Calculate $x = F^{-1}(b)$, either analytically or by searching the table. (Note that F^{-1} implies an inverse function; meaning we are looking for the value of x that corresponds to the probability $F(x)$.)

Then x is a random sample derived from the distribution F , and with probability b that the value of the sampled variable is less than x .

Sometimes the probability distribution makes sense over only a subset of the range of values for which the distribution is defined. For example, if the random number represents the thickness of a pad, then only positive random values make sense in a simulation. In that case, a truncated distribution can be used with random values outside the desired interval discarded. For a truncated distribution, the random number generation procedure described above is modified as follows: If x_1 and x_2 are the ends of the desired interval, then the "Random Number" described in step 1 above is drawn from a uniform distribution between $F(x_1)$ and $F(x_2)$ instead of from a uniform distribution between 0 and 1.

Methods for generating commonly used distributions are described in the following sections.

F.3.2.2 Uniform Distribution

In a uniform distribution, all possible values of the parameter are equally likely to occur. Pseudo-random number generators (PRNGs), by their nature, provide output values fitting a uniform distribution. A typical PRNG produces values between 0 and 1. A simple example where a Uniform Distribution might be appropriate is in modeling a scheduled maintenance task. For example, suppose an engine inspection is scheduled to take place after 500 hours of service, but before 550 hours. If the inspection is equally likely to occur at any time in the interval, a Uniform Distribution can be used to model the inspection times. This can be included in a Monte Carlo simulation by using mathematical steps similar to those shown below.

1. Sample a Random Number.
2. Multiply the above Random Number by 50 to convert it to a corresponding random value within the allowed 50-hour inspection interval.
3. Assign a specific Inspection Time by adding the above value to the minimum 500-hour Inspection Time.
4. The results of the above three steps can be mathematically expressed as $\text{Inspection Time} = 500 + (50 \times \text{"Random Number"})$.

F.3.2.3 Normal Distribution

A graph of the probability density function for a normal distribution shows the traditional bell-shaped curve that has found application in many fields. Two parameters, the mean and the standard deviation, define the normal distribution. The normal distribution is symmetric, meaning that it is equally likely for the value of a random variable to be X% greater than the mean as it to be X% less than the mean. With a normal distribution, the mean is also the most likely value. Additionally, the further a specific value is from the mean, the smaller the probability density function is at that value. A graphical depiction of the probability density function for the normal distribution is shown in Figure F4.

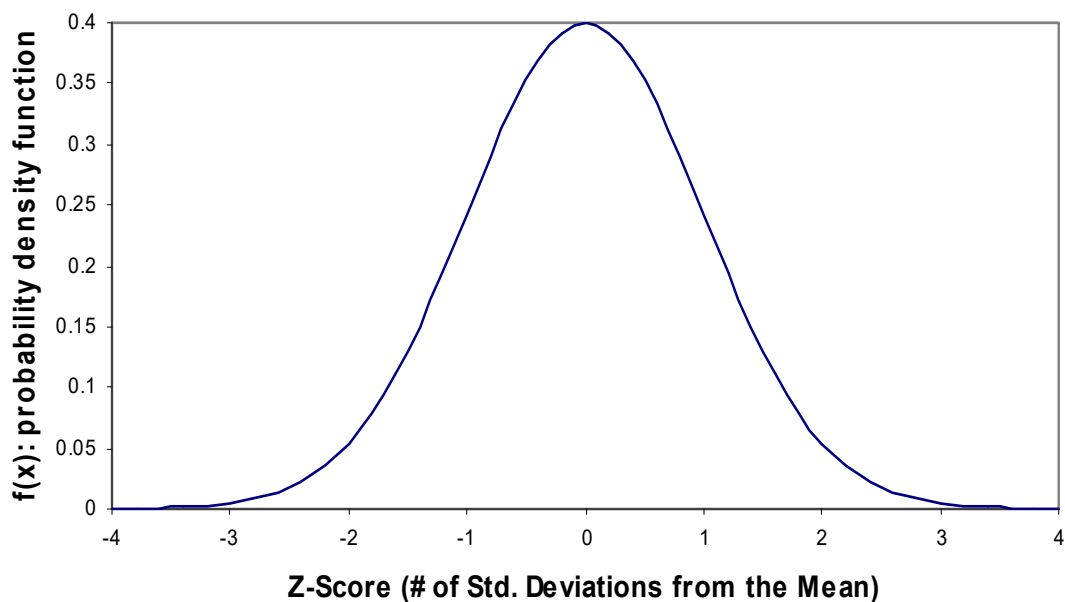


Figure F4 - Standard normal distribution - probability density function

For most applications of the normal distribution, including Monte Carlo modeling, it is more convenient to use the cumulative distribution function than the probability density function. A graphical depiction of the cumulative density function for the normal distribution is shown in Figure F5.

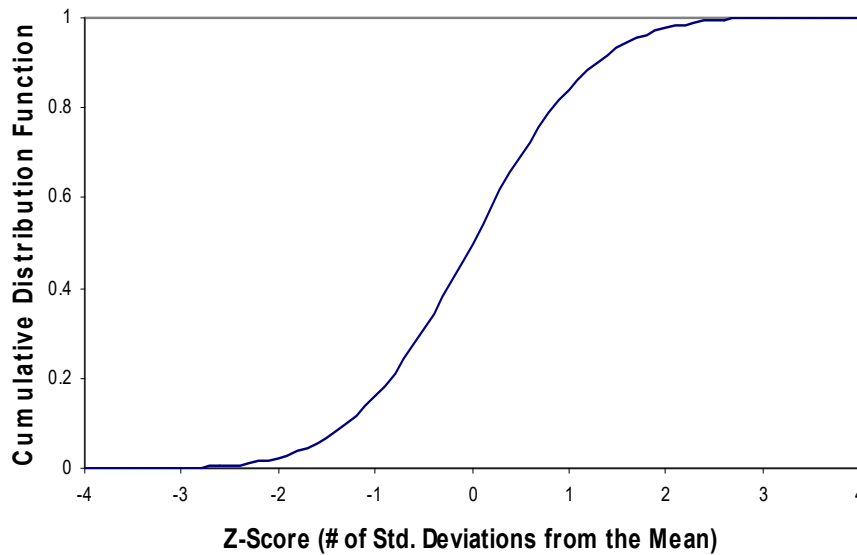


Figure F5 - Standard normal distribution - cumulative density function

The mathematical equation for the cumulative distribution function for the normal distribution involves an integral that has no closed-form solution. To ease calculations, probability values have been tabulated for a “standardized” normal distribution (which has a mean of 0 and a standard deviation of 1). Tables of the “Standard Cumulative Normal Distribution Function” can be found in any statistics textbook. In these tables, cumulative probability values are given as a function of “Z-Score.” Note that both Figure F4 and Figure F5 also use Z-Score as the X-axis variable. The use of the Z-Score parameter is necessary when relying on a Normal Distribution table in performing calculations. Although this is not a necessary step when using computer software packages (as Standard Normal PRNGs are often available), the Z-Score concept is used here for illustration.

The Z-Score provides a method to translate a normal distribution with arbitrary mean and standard deviation values to the nominal normal distribution with mean 0 and standard deviation 1. This translation is performed via Equation F1.

$$\text{Z-Score} = (x - \text{mean}) / \text{standard deviation} \quad (\text{Eq. F1})$$

Thus, for a normal distribution with a specific mean and standard deviation, there is a unique Z-Score for each unique value of the random variable x .

Solving the above expression for the random variable x ,

$$x = [(\text{Z-Score}) * (\text{standard deviation})] + \text{mean} \quad (\text{Eq. F2})$$

When one of the parameters in a Monte Carlo simulation is normally distributed, the following steps are used to randomly generate values for that parameter.

1. Sample a Random Number.
2. Assign that random number as the cumulative probability value, and determine the corresponding Z-Score (e.g., from a Normal Distribution Table).
3. Using Equation F2, assign a value of “ x ” based on the assigned Z-Score.

As an example, consider a case where a Monte Carlo simulation includes Drive Shaft Diameter as a parameter, and that Drive Shaft Diameter is normally distributed with a mean of 10 cm and a standard deviation of 0.05 cm. Table F1 shows the results of ten sampling iterations using the steps described above.

Table F1 - Drive shaft diameter distribution example

Simulation of Shaft Diameters, Mean = 10.0, Std. Deviation = 0.05			
Iteration	Random Number	Z-Score	Shaft Diameter $x = (Z\text{-Score})(0.05) + (10.0)$
1	0.437	-0.158	9.992
2	0.644	0.369	10.019
3	0.517	0.042	10.002
4	0.210	-0.807	9.960
5	0.580	0.202	10.010
6	0.602	0.259	10.013
7	0.293	-0.546	9.973
8	0.257	-0.651	9.967
9	0.177	-0.927	9.954
10	0.129	-1.132	9.943

An important feature of the normal distribution is that parameter values can theoretically take on values from negative infinity to positive infinity. This “feature” of the normal distribution can, in some instances, mean that a numerical value which is physically impossible is modeled to have a small (but theoretically possible) probability. For example, a Z-Score of -200 or smaller results in a negative Drive Shaft Diameter in the preceding example. To prevent such physically impossible values from being simulated by the Monte Carlo model, it is good practice to use a truncated normal distribution. Just as with the normal distribution, the truncated normal distribution is defined in terms of a mean value and standard deviation. However, a truncated normal distribution also establishes a minimum possible value and a maximum possible value. By appropriately establishing these minimum and maximum values, no physically impossible parameter values will be simulated by the Monte Carlo model.

F.3.2.4 Lognormal Distribution

The lognormal distribution is closely related to the normal distribution, as might be deduced from its name. For the lognormal distribution, instead of the random variable being normally distributed, it is the logarithms of the random variable that are normally distributed. This is illustrated in Figure F6, which shows the traditional bell-shaped curve with $\log(x)$ used as the x-axis variable.

Figure F7 shows a re-plot of the Figure G6 data, using x instead of $\log(x)$ as the x-axis variable. Now, instead of a symmetric bell-shaped curve, the right side tail stretches much further to the right. This is often appropriate when modeling material strength data or component lifetime data, where the highest strength or lifetime can be orders of magnitude greater than the mid-range (or typical) value.

The lognormal distribution has another characteristic that distinguishes it from the normal distribution. Since 10^x takes on positive values for any value of x , the lognormal distribution always has a theoretical minimum value of zero. This can make it a better fit for parameters that cannot physically take on negative values. For example, component lifetimes cannot be less than zero. This characteristic of the lognormal distribution is one reason that the lognormal distribution is often used as a reliability model. However, the lognormal distribution also has the characteristic that the failure rate (i.e., the hazard function) increases from 0 to reach a maximum and then decreases, approaching 0 as x approaches infinity. For wearout failure distributions, the lognormal function gives erroneous values for the hazard function for large values of x .

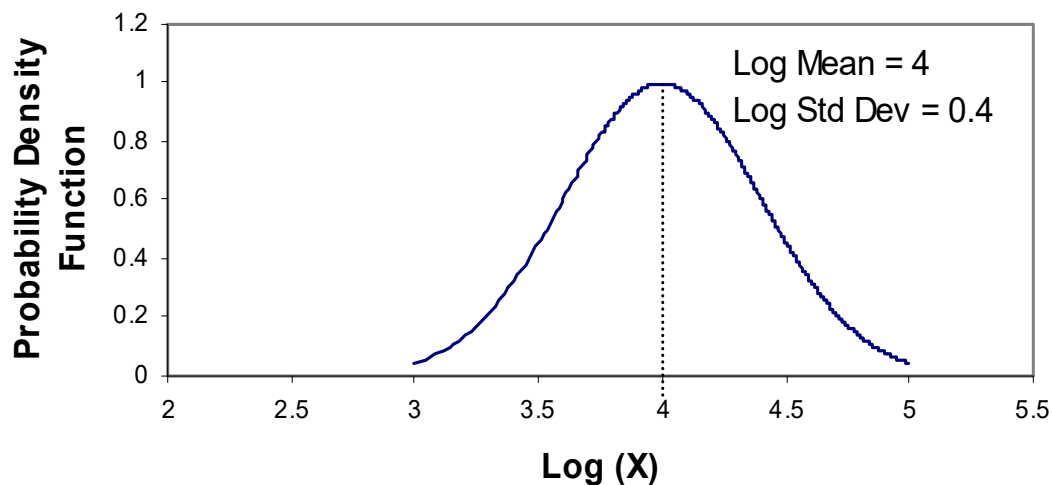


Figure F6 - Lognormal distribution - probability density function versus $\log(x)$

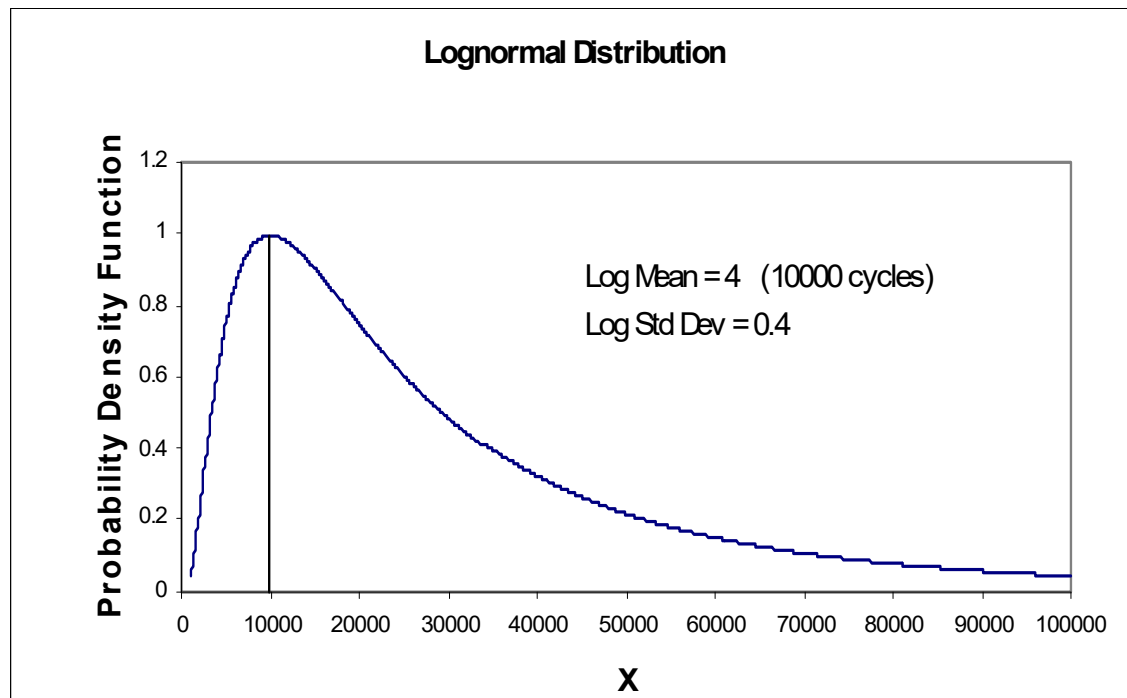


Figure F7 - Lognormal distribution - probability density function versus x

Both Figures F6 and F7 depict the probability density function for a specific lognormal distribution. However, as illustrated in the earlier examples, it is the cumulative distribution function (cdf) that is used in a Monte Carlo model. Figures F8 and F9 show the cumulative probability function for the lognormal distribution depicted in Figure F6. Figure F8 uses $\log(x)$ as the x-axis variable, resulting in an s-shaped curve similar to the normal distribution in Figure F5. Figure F7 plots x values directly, and the curve shape is distinctly different.

With any cumulative probability plot, values on the y-axis go from a minimum value approaching zero to a maximum value approaching one. For the lognormal distribution, the y-values approach zero as $\log(x)$ values approach negative infinity (and x values approach zero). A y-value can approach the maximum theoretical value of one as $\log(x)$ values (and x values) approach infinity. For each possible y-value, there is a unique $\log(x)$ value and, consequently, a unique x value.

When one of the parameters in a Monte Carlo simulation is lognormally distributed, the following steps are used to randomly generate values for that parameter.

1. Sample a Random Number.
2. Assign that Random Number as the cumulative probability value (analogous to the y-axis value in Figure F7).
3. Determine the x value that corresponds to that cumulative probability (analogous to the x-axis value in Figure F7). This can be accomplished using the Z-Score technique described in the Normal Distribution section, but most software packages have the lognormal function available as a mathematical operation and can make the calculation directly.

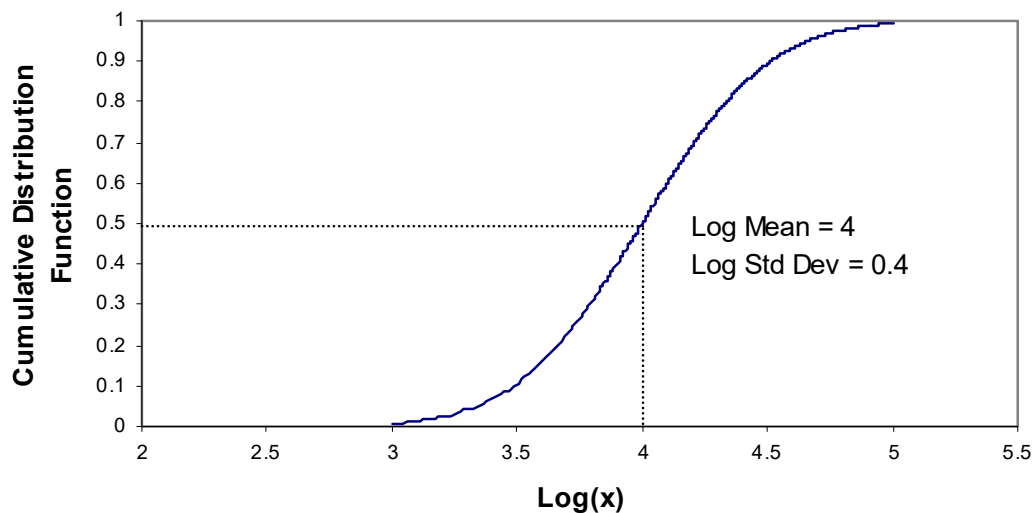


Figure F8 - Lognormal distribution - cumulative density function versus $\log(x)$

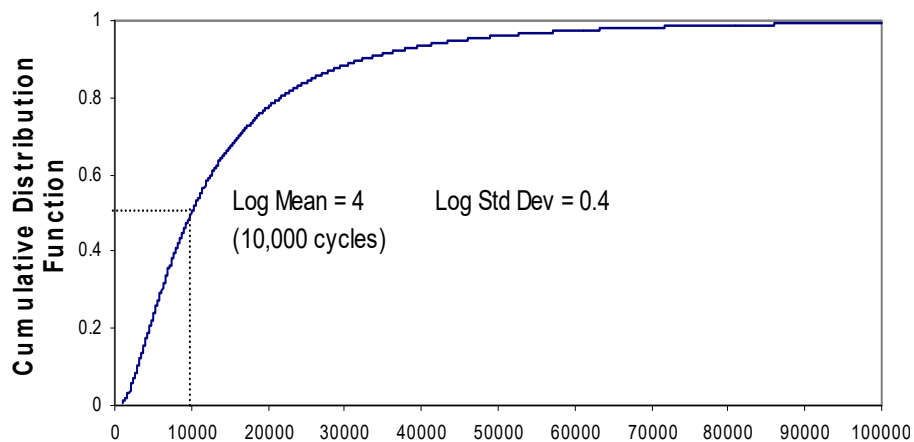


Figure F9 - Lognormal distribution - cumulative density function versus x

As an example, consider a turbine disk where the crack propagation life can be modeled as a lognormal distribution as shown in Figure F8. Specifically, the mean of the logarithm of life values is 4 (i.e., 10,000 cycles) and the standard deviation of the logarithm of life values is 0.4. Table F2 shows the results of ten sampling iterations using the steps described above.

Table F2 - Simulation of crack propagation lives, lognormal distribution, log mean = 4.0, log standard deviation = 0.4

Iteration	Random Number	Z-Score	Log Life = (Z-Score)(0.4) + 4.0	Life = $10^{\text{Log Life}}$
1	0.324	-0.458	3.817	6558
2	0.077	-1.427	3.429	2687
3	0.278	-0.588	3.765	5818
4	0.079	-1.411	3.436	2727
5	0.479	-0.053	3.979	9523
6	0.314	-0.486	3.806	6394
7	0.881	1.182	4.473	29702
8	0.002	-2.847	2.861	726
9	0.514	0.035	4.014	10326
10	0.723	0.593	4.237	17260

F.3.2.5 Weibull Distribution

The Weibull distribution has found wide usage in the reliability field due to its great flexibility in modeling life distributions. It can conveniently model failure mechanisms that exhibit infant mortality as well as those that exhibit late age mortality. Like the lognormal distribution, it models only non-negative random variables and thus is useful for reliability applications such as modeling component life times. A complete description of the Weibull distribution and its uses can be found in Appendix E. The Weibull distribution is defined by two parameters, the characteristic life η and the slope β . The cumulative distribution function for the Weibull distribution is written as:

$$F(t) = 1 - e^{-(t/\eta)^\beta} \quad (\text{Eq. F3})$$

where:

$F(t)$ = probability of failure prior to age t

η = Weibull characteristic life

β = Weibull slope

t = service life or age

A typical use of the Weibull distribution in a Monte Carlo simulation is to assign random failure times to a specific component. To facilitate this, Equation F3 can be rearranged to solve for t :

$$t = \eta [-\ln(1-F(t))]^{1/\beta} \quad (\text{Eq. F4})$$

Random failure times can then be generated using the following steps.

1. Sample a Random Number from the range 0 to 1.
2. Assign that Random Number as the cumulative probability value $F(t)$.
3. Determine the t value that corresponds to that cumulative probability by using Equation F4.

As an example, consider a ball bearing with a Weibull life distribution with $\eta = 18000$ hours and $\beta = 1.5$. Table F3 shows the results of 10 sampling iterations using the steps described above.

**Table F3 - Simulation of bearing failure times, Weibull distribution,
Weibull char life = 18000, slope = 1.5**

Iteration	F(t) = Random Number	$t = 18000 [-\ln(1-F(t))]^{1/1.5}$
1	0.869	28859
2	0.952	37764
3	0.729	21499
4	0.112	4346
5	0.998	60693
6	0.188	6313
7	0.459	13016
8	0.499	14078
9	0.800	24754
10	0.478	13500

F.3.2.6 Exponential Distribution

The exponential distribution is fully defined in terms of the single parameter λ . It is equivalent to a special case of the Weibull distribution, where the Weibull slope β is equal to 1 and λ is equal to $1/\eta$. When used as a reliability model, the exponential distribution depicts a failure mechanism having a constant hazard rate. This means that the risk of failure per unit time is constant with component age. This is often a useful model for non-inherent failure causes, such as foreign object damage, extreme weather, maintenance errors, etc.

The cumulative distribution function for the exponential distribution is written as:

$$F(t) = 1 - e^{-\lambda t} \quad (\text{Eq. F5})$$

where:

$F(t)$ = probability of failure prior to age t

λ = hazard rate (failures per unit time)

t = service life or age

A typical use of the exponential distribution in a Monte Carlo simulation is to assign random failure times when the mechanism is judged to be independent of product age. To facilitate this, Equation F5 can be rearranged to solve for t as shown in Equation F6.

$$t = [-\ln(1-F(t))] / \lambda \quad (\text{Eq. F6})$$

Random failure times can then be generated using the following steps.

1. Sample a Random Number.
2. Assign that Random Number as the cumulative probability value $F(t)$.
3. Determine the t value that corresponds to that cumulative probability by using Equation F6.

As an example, consider engine bird ingestion events, where service history indicates an occurrence rate of one event per 400000 flight hours, or $\lambda = 2.5\text{E-}06$. Table F4 shows the results of ten sampling iterations using the steps described above.

Table F4 - Simulation of bird ingestion events, exponential distribution, $\lambda = 2.5\text{e-}06$ events per hour

Iteration	F(t) = Random Number	$t = (-\ln(1-F(t))) / 2.5\text{E-}06$
1	0.451	239726
2	0.766	581384
3	0.490	269519
4	0.634	402245
5	0.324	156349
6	0.447	237189
7	0.934	1089358
8	0.445	235543
9	0.063	25834
10	0.337	164219

F.4 EXAMPLES

F.4.1 Interference/Clearance of Shaft - Bore Fit

Monte Carlo simulation can be used to calculate the probability of encountering an interference condition when assembling a shaft into a bore. For example, consider a shaft with a diameter that is normally distributed, and a bore with a diameter that is uniformly distributed. The parameters of the distributions are shown in the Table F5. The cdf for each component is graphically shown in Figures F10 and F11.

Table F5 - Input parameters for shaft and bore example

Shaft Normal Distribution	Bore Uniform Distribution
$\mu_x = 1.9990$ cm	$y_{\min} = 2.000$ cm
$\sigma_x = 0.0010$ cm	$y_{\max} = 2.002$ cm

A simple comparison of the shaft nominal diameter (1.999 cm) to the bore nominal diameter (2.001 cm) shows that the nominal clearance is 0.002 cm. However, it is also clear that with a +2 sigma shaft (2.0010 cm) and minimum bore (2.000 cm), interference will occur. Monte Carlo simulation can be used to calculate the probability of selecting both a large diameter shaft and a small diameter bore such that an interference condition will prevent proper assembly.

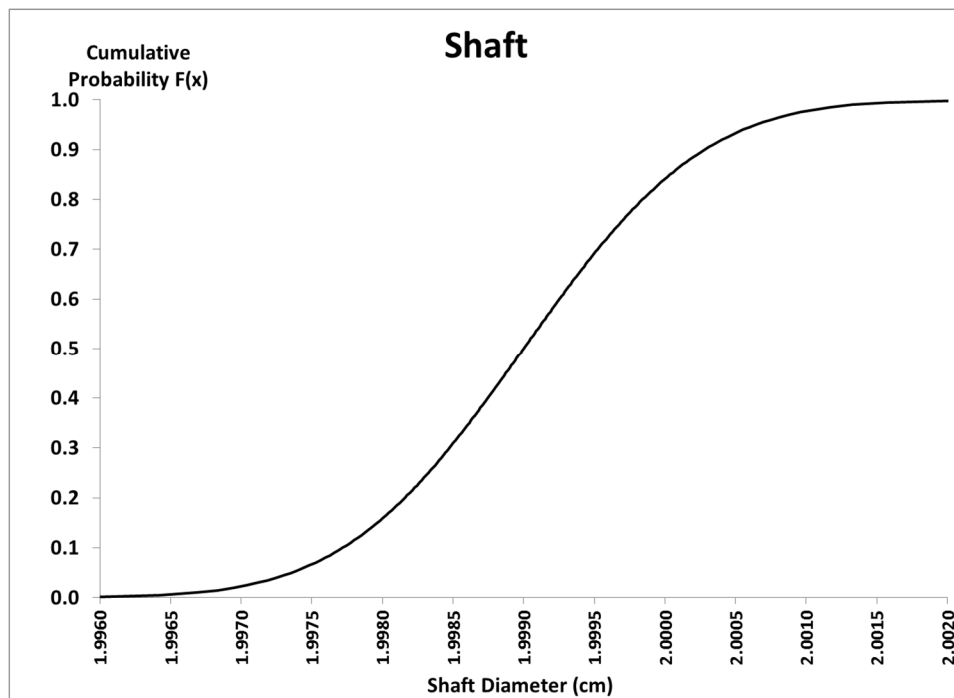


Figure F10 - Cumulative distribution function for shaft, normal distribution, mean = 1.9990 cm, standard deviation = 0.0010 cm

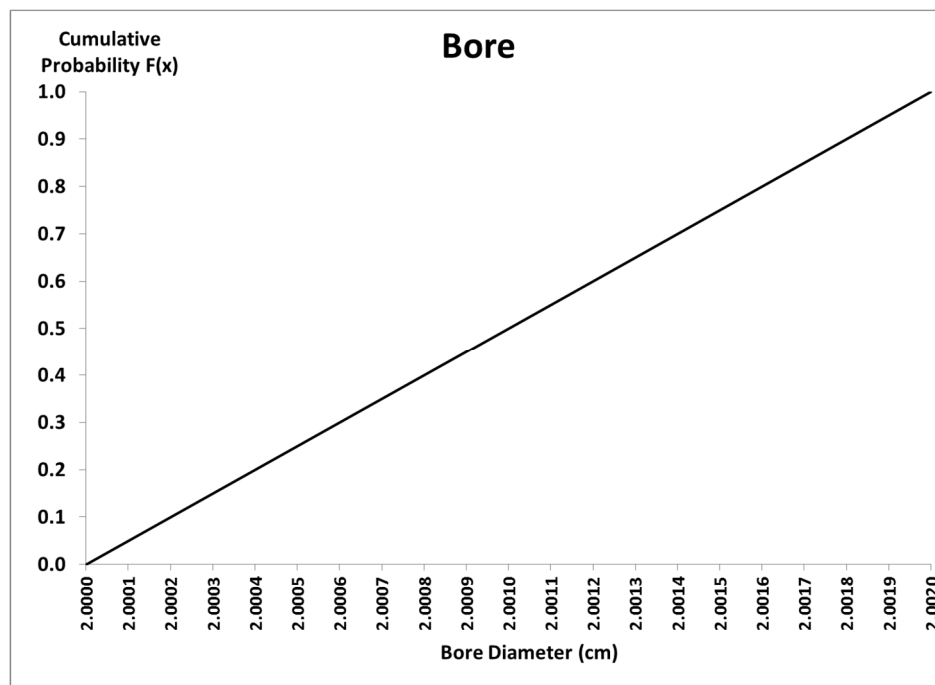


Figure F11 - Cumulative distribution function for bore, uniform distribution, $y_{min} = 2.000$ cm, $y_{max} = 2.002$ cm

Table F6 shows the various steps and calculations which comprise the Monte Carlo simulation. Column A tabulates 20 different Random Numbers between 0 and 1 (which can be obtained from a table of random numbers or a computer random number generator). Each Random Number represents one trial in the simulation. Column B tabulates specific shaft diameters for each trial. The shaft diameter value for a specific trial is obtained by reading the diameter value on the x-axis that corresponds to a cumulative probability, $F(x)$, equal to the random number. Similarly, Columns C and D tabulate 20 additional Random Numbers and the corresponding random bore diameters. Column E then tabulates the clearance or interference between the shaft and bore by subtracting Column B from Column D.

Out of 20 trials, the simulation produced one interference condition (trial number 11). Thus, based on the Monte Carlo simulation, it can be concluded that the probability of a shaft-bore interference condition is 1 in 20, or 0.05. The example used a small number of trials (20) in order to make it easier to illustrate the procedure. It is normally necessary to run many more trials in order to obtain accurate results. The same problem analyzed using 500 trials produced 24 interference events, or a probability of 24 in 500, or 0.048.

Table F6 - Shaft and bore example, simulation of shaft - bore interference

	A	B	C	D	E
Trial No.	Random Number	Corresponding Shaft Diameter	Random Number	Corresponding Bore Diameter	Clearance (Bore - Shaft)
1	0.8967	2.0003	0.3635	2.0007	0.0005
2	0.9566	2.0007	0.9681	2.0019	0.0012
3	0.2000	1.9982	0.8688	2.0017	0.0036
4	0.6424	1.9994	0.3164	2.0006	0.0013
5	0.9630	2.0008	0.5386	2.0011	0.0003
6	0.4706	1.9989	0.2547	2.0005	0.0016
7	0.0083	1.9966	0.1888	2.0004	0.0038
8	0.7847	1.9998	0.3647	2.0007	0.0009
9	0.6342	1.9993	0.8283	2.0017	0.0023
10	0.5859	1.9992	0.7040	2.0014	0.0022
11	0.8992	2.0003	0.0211	2.0000	-0.0002
12	0.7792	1.9998	0.2127	2.0004	0.0007
13	0.8967	2.0003	0.3635	2.0007	0.0005
14	0.9566	2.0007	0.9681	2.0019	0.0012
15	0.2000	1.9982	0.8688	2.0017	0.0036
16	0.6424	1.9994	0.3164	2.0006	0.0013
17	0.9630	2.0008	0.5386	2.0011	0.0003
18	0.4706	1.9989	0.2547	2.0005	0.0016
19	0.0083	1.9966	0.1888	2.0004	0.0038
20	0.7847	1.9998	0.3647	2.0007	0.0009

F.4.2 Engine Time-on-Wing

Monte Carlo simulation can be used to calculate the expected time-on-wing for engines subject to multiple removal causes. For the simple example discussed here, engines can be removed for three distinct causes.

1. Unscheduled removal due to an inherent engine failure.
2. Unscheduled removal for a non-inherent cause (e.g., foreign object damage).
3. Scheduled removal as required by a stated overhaul period.

Each of the three causes must be defined by a cumulative probability distribution. For this example, the following distributions are assigned.

1. Unscheduled removal due to an inherent engine cause (e.g., turbine blade failure): Weibull distribution with Characteristic Life = 4000 hours and Slope = 1.2.
2. Unscheduled removal due for a non-inherent cause (e.g., bird ingestion): exponential distribution with hazard rate (λ) = 0.0001 per hour.
3. Scheduled removal as required by a stated overhaul period: uniform distribution with minimum = 2900 hours and maximum = 3000 hours.

For each iteration in a Monte Carlo simulation, a “Potential Time-on-Wing” value is generated for all three potential removal causes. These values are generated as shown in F.3.2.5 (Weibull distribution), F.3.2.6 (exponential distribution), and F.3.2.2 (uniform distribution). The “Actual Time-on-Wing” for that iteration is simply the earliest (lowest time) of the three “Potential Time-on-Wing” values. Table F7 shows the results of twenty iterations.

F.4.3 Using a Risk Simulation Program when a Field Problem is Defined - Using Part Lives, Inspections, and a Fix Incorporation Schedule

This section will discuss three progressive Monte Carlo risk simulation runs for a field problem where parts can crack and propagate to failure:

1. No Corrective Action Field Management Scenario - no inspections or fix.
2. Same input for #1, plus an inspection plan using shop visit rate.
3. Same as #2, plus a field fix incorporation plan.

Table F7 - Simulation of engine time-on-wing

	A	B	C	D	E	F	G	H
	Inherent Engine Removals		Non-Inherent Engine Removals		Scheduled Engine Overhaul			
Iteration Number	Random Number	Potential Time-on-Wing *	Random Number	Potential Time-on-Wing **	Random Number	Potential Time-on-Wing ***	Simulated Time-on-Wing (Minimum from Columns B, D, and F)	Removal Reason
1	0.963096469	10816.7	0.781752813	15221.3	0.805702366	2980.6	2980.6	O/H
2	0.197616409	1133.3	0.002075024	20.8	0.590138659	2959.0	20.8	Non-Inh
3	0.939515647	9449.0	0.194492583	2162.8	0.32297997	2932.3	2162.8	Non-Inh
4	0.644434607	4113.2	0.20360458	2276.6	0.811905935	2981.2	2276.6	Non-Inh
5	0.91706761	8554.3	0.732323052	13179.7	0.356015997	2935.6	2935.6	O/H
6	0.489709299	2874.9	0.646352546	10394.5	0.039680861	2904.0	2874.9	Inh
7	0.371854518	2113.1	0.194551724	2163.6	0.903805965	2990.4	2113.1	Inh
8	0.10928106	663.1	0.460614998	6173.3	0.911227016	2991.1	663.1	Inh
9	0.284614241	1607.7	0.407786171	5238.9	0.079309434	2907.9	1607.7	Inh
10	0.149396228	876.8	0.431678637	5650.7	0.72722465	2972.7	876.8	Inh
11	0.066242867	428.6	0.782524203	15256.7	0.38152307	2938.2	428.6	Inh
12	0.193023246	1108.8	0.892626776	22314.4	0.698895725	2969.9	1108.8	Inh
13	0.63068744	3987.0	0.192675773	2140.3	0.480091813	2948.0	2140.3	Non-Inh
14	0.865066411	7136.0	0.028544632	289.6	0.548153891	2954.8	289.6	Non-Inh
15	0.810531595	6113.0	0.442122373	5836.2	0.295148533	2929.5	2929.5	O/H
16	0.485162473	2843.2	0.991977351	48254.9	0.420893922	2942.1	2843.2	Inh
17	0.336765474	1905.2	0.585047639	8795.9	0.964186319	2996.4	1905.2	Inh
18	0.370164373	2102.9	0.595638839	9054.5	0.980361006	2998.0	2102.9	Inh
19	0.7428252	5161.9	0.497612743	6883.8	0.266078692	2926.6	2926.6	O/H
20	0.68860395	4548.4	0.990716423	46795.1	0.037321199	2903.7	2903.7	O/H
	* $t = 4000 [-\ln(1-F(t))]^{1/1.2}$, where F(t) is given in Column A							
	** $t = (-\ln(1-F(t))) / .0001$, where F(t) is given in Column C							
	*** $t = 2900 + [F(t) * (3000 - 2900)]$, where F(t) is given in Column E							

First, a risk simulation model must be developed. All the desired outputs must then be defined, and from that the risk analyst can determine what inputs are required. The model below displays a variety of possible inputs into the risk analysis model.

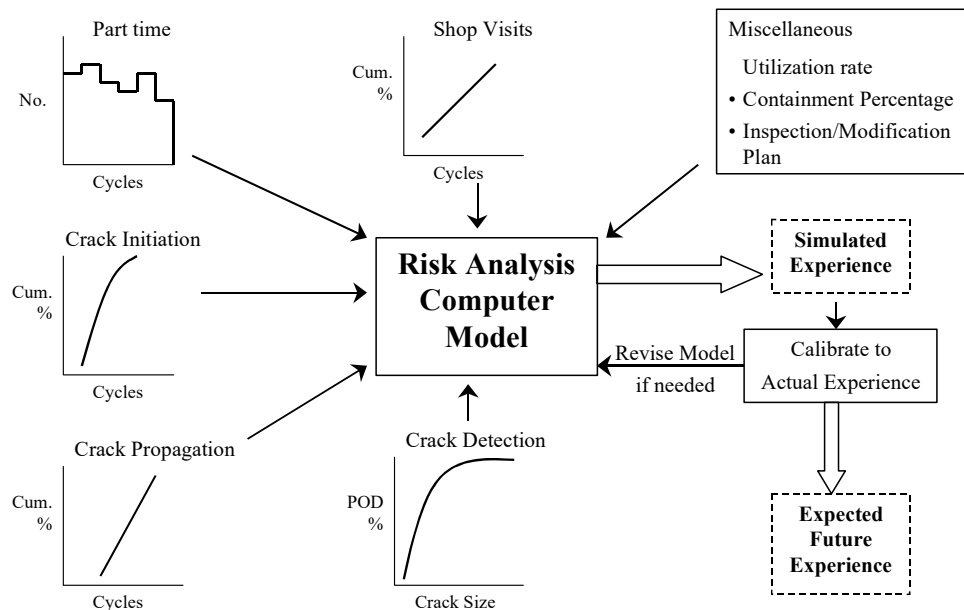


Figure F12 - Simulation model for component subject to crack initiation and propagation

F.4.3.1 Model Development

An important part of developing the simulation program is identifying and defining the applicable parameters. The analyst must obtain or define the needed probability distributions, such as:

- Current ages (hours or cycles) of fielded parts.
- Utilization rates (hours or cycles per month) for fielded parts.
- Crack initiation life distribution for fielded parts.
- Crack propagation rates for fielded parts.

Since there is an entire fleet of parts to consider, one of the inputs to the Monte Carlo model is a list or histogram defining the quantity and ages of suspect parts in the fleet. The simulation then “flies” this fleet of parts through time based on the expected utilization rate or distribution (e.g., hours per month). Each part is run until a crack is found, it fails in service, it reaches its assigned life limit, or a typical lifetime exposure period passes, whichever comes first. The simulation program should track the number of failures, as well as the calendar time of the failures. If a part is simulated to retire at its life limit or fail in service, it is then replaced with another part to complete the exposure period. After all iterations of all suspect parts have run, the simulation can calculate the expected number of failures and when they occurred.

F.4.3.2 Calibration - An Important First Step to a Good Model

A risk simulation model will be a good predictor of future events only if it can accurately predict the current field experience. For example, suppose there have been five cracked parts found with no failures due to this problem, and, as part of the input, calculated crack initiation and propagation lives are provided. Assume that the simulation predicts that there should have been 15 cracks found to date. One or more of the inputs must be adjusted to lower the prediction to five cracks to match the field experience. If it is agreed that all inputs, other than the lives, are reliable, then the crack initiation life distribution is too conservative and needs to be increased until it predicts just five cracks found to date. Similarly, if the simulation under-predicts the number of cracks, the crack initiation life distribution needs to be decreased. If the simulation also predicts more than one failure (and, as mentioned, none have occurred), then the crack propagation life distribution should be increased until one (assumed) failure is predicted. If less than one failure is predicted to date, either the propagation life should be decreased until one (assumed) failure is predicted (conservative approach) or use the life as is, whichever approach seems more appropriate. Changing model parameters to calibrate the model should be done with care, and known failure behavior should not be compromised just to make the simulation answer match exactly with a known quantity. The randomness of the process assures uncertainty in the simulation result. The Poisson distribution can be helpful in calculating the probability of the actual outcome given the prediction and thus serve as a guideline to whether to revise the simulation inputs for better calibration.

The technique described in the previous paragraph provides a calibration under the assumption that all other inputs, except for the lives, are accurate. Even slight input inaccuracies (such as inspection reliability or suspect fleet size) may have an impact on the risk analysis results; but, if adequate care is taken in their definition, calibration is usually a matter of adjusting the lives. Once the simulation has been calibrated, it is ready to predict future events for various scenarios in search of one that yields acceptable risk of part failure and minimizes the impact of the airline operations.

Here is an example that is used for three risk simulation scenarios, the first of which is No Corrective Action.

F.4.3.3 No Corrective Action

The typical baseline risk analysis scenario is, "What if the suspect parts are allowed to run its lifetime exposure with no corrective action?" This may include replacement with more suspect parts or part retirement without continued risk.

There are 32 suspect parts, with ages ranging from 100 to 2200 cycles. Their calculated crack initiation life does not fit a Weibull distribution, but it can be defined by a set of pairwise points. Select $F(t)$ s and their corresponding t values to define the distribution, especially at the lower tail. For this specific example, 99% of parts will have initiation ages from 3800 to 32500 cycles. Crack propagation life is defined by a Weibull distribution with a slope of 7.1 and a characteristic life of 537 cycles. An additional constraint on the propagation life is defined: specifically, there is a minimum propagation life of 204 cycles. The sum of the median initiation life and the median propagation life is 19800 cycles, so the median part will fail at 19800 cycles of operation. The parts accrue 65 cycles per month. The simulation results are 6.7 failures in 20 years (lifetime exposure for this part), with the first failure expected after 11 years.

Using interpolation and pairwise points from the plot, such as $(t_1, F(t_1))$, $(t_2, F(t_2))$, . . . , the analyst can use the set of points in the simulation to represent the crack initiation life.

F.4.3.4 Field Management Plan with Inspections

To simulate this scenario, the analyst must simulate the next shop visit, or, other maintenance opportunity, leading to a part inspection. The relationship between crack size and probability of detection (POD) can be used, if available. If not, a constant POD is used. In this example, a 90% on-wing inspection reliability is assumed. If the part is simulated not to be cracked or found to be cracked but not found by inspection, it goes to the next inspection opportunity, adding hours/cycles to the part. If it is found cracked, the program calculates the calendar time from simulation start, and bookkeeps the crack there. If it is simulated that the part fails before the next inspection, the same bookkeeping is done for failures. In either case, it is then replaced with another suspect part (assuming continuing risk with new parts). After all iterations have run for all suspect parts, the program will sum the expected number of failures and cracks to be found and in what timeframes. The inspection plan is then varied to determine the effect on the expected number of failures. Through this process, an inspection plan can be developed that minimizes the failures to an acceptable level while controlling impact on the customer.

For example, the first option may be to perform inspections every 500 cycles, starting at 4000 cycles for the first inspection. The expected number of failures is 1.0, and 6.1 cracks found by inspections, with the first crack found in 11.5 years. If the company has defined an acceptable risk factor of 0.50 failures, the inspection plan is unacceptable and needs to be revised. With the same initial inspection of 4000, but re-inspecting every 350 cycles, the simulation yields a risk factor of 0.49 failures and 6.7 detected cracks in 20 years. However, 350 cycles is inconvenient for the operator, so the re-inspection interval is set at 250 cycles. The risk factor for this inspection plan is 0.18 failures and 7.1 detected cracks. Remember that this field management plan does not take into account any fix or repair.

F.4.3.5 Field Management with a Repair/Replacement Incorporation Schedule

To simulate for this scenario, the analyst must simulate the next opportunity for replacing, or repairing, the part. The simulation checks for cracks, replacing/repairing the part at availability, and counting and dating the cracks and failures. For example, the risk analyst defines the corrective action as a newly designed part with adequate life to meet the formally approved life limit. It will be available in 2 years, and is installed at next shop visit, which occurs every 2000 to 5000 cycles. The inspection plan used above can be revised to fit in with the replacement schedule.

F.5 SIMULATION LANGUAGES

There are many choices available when selecting a computer software package or programming language for Monte Carlo simulation. These choices include general purpose programming languages (for example, Fortran, Visual Basic, C/C++, Java, MatLab, or R), spreadsheet software such as Microsoft Excel, and special purpose simulation software such as @Risk and Crystal Ball.

F.6 CAUTIONS AND LIMITATIONS

Accuracy of results depends on the accuracy and completeness of the system model. (There are always more parameters in a real life system than can be included in a model).

Accuracy of results also depends on the properties of the PRNG. No "random" number generators are truly random; simulating safety events often uses parameter distributions where the extreme tails of the distribution are important. Thus, it is important that the PNRG be able to properly model these tails. The simulation should be run enough times that the system failures being modeled show up in the results at least 10 times. Thus, rare events will require many tens of thousands (or more) trials to obtain failures in 10 trials. Additionally, demonstrating that system unreliability to very small numbers (for example, less than $1.0E-9$) can be expected to require billions of simulations, or use of a simulation that forces evaluation at the distribution tails and then corrects to the full cdf.

APPENDIX G - RELIABILITY GROWTH MODELING

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

G.1 SCOPE

This appendix presents the tools and methods associated with reliability growth modeling.

G.2 RELIABILITY GROWTH MODELING

Reliability growth modeling characterizes the improvement in a product's reliability that can occur as test or service experience is used as an input to the product improvement process. These product improvements are typically changes to the product design, but they can also include improvements to the manufacturing process, changes to operating procedures, or changes to maintenance procedures.

In the 1970s, the Army Material Systems Analysis Agency (AMSAA) developed the Crow-AMSAA reliability growth model which can be used both as monitoring tools and prediction tools. During development testing or early field service, reliability growth is monitored by plotting cumulative MTBF (or cumulative number of incidents) versus cumulative operating time on log-log paper. This provides not only a measure of current reliability, but also an indication of the changes in failure rate. Operating time can be defined as whatever time units are most appropriate to assessing the failure mode (such as hours, cycles, etc.).

G.2.1 Army Material Systems Analysis Agency (Crow-AMSAA) Model

Reliability growth modeling was originally conceived as a metric for use during the product development phase. The Crow-AMSAA metric uses log-log graph paper, and plots the number of cumulative product failures versus cumulative test time. For many product development programs, this data forms a straight line on log-log paper. An example is shown in Figure G1.

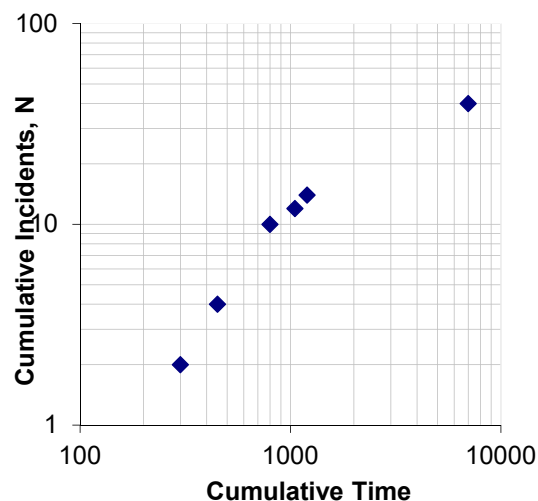


Figure G1 - Incidents versus time plot

Equation G1, first documented by the Army Material Systems Analysis Agency , provides a useful mathematical equivalent to the graphical representation.

$$N(t) = \lambda t^\beta \quad (\text{Eq. G1})$$

where:

$N(t)$ = cumulative events at time t

λ = scale parameter (intercept)

β = growth parameter (slope)

The results of Equation G1, when plotted on log-log scale will be a straight line. This can be shown through the following derivation:

$$\log[N(t)] = \log(\lambda t^\beta) \quad (\text{Eq. G2})$$

$$= \log(\lambda) + \log(t^\beta) \quad (\text{Eq. G3})$$

$$= \beta \log(t) + \log(\lambda) \quad (\text{Eq. G4})$$

Equation G4 is of the form $y = mX + b$, which is a straight line.

The growth parameter (slope) characterizes whether a failure rate is decreasing, constant or increasing, as shown in Figure G2.

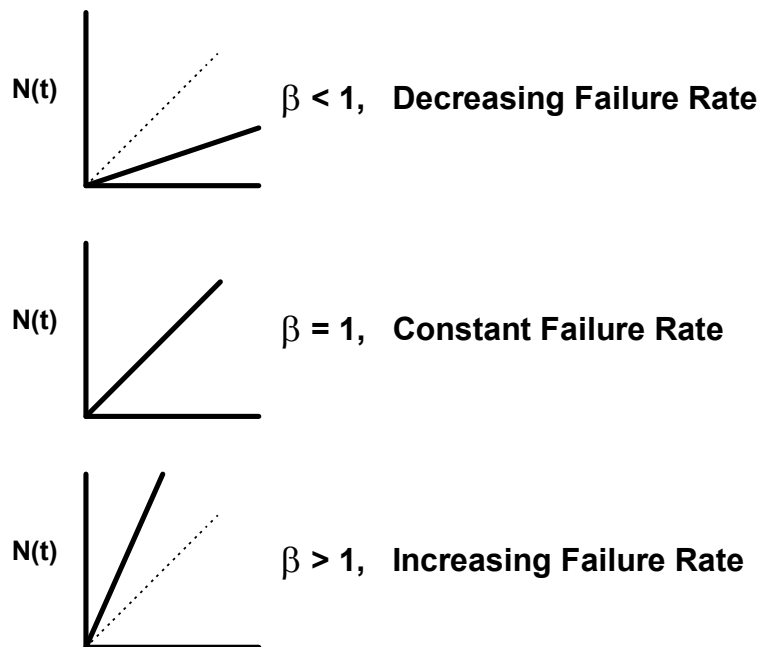


Figure G2 - Growth slope characterizations

The Growth Trend can be formulated many ways. The following equations identify some of these possibilities:

$$\text{Cumulative Events:} \quad N(t) = \lambda t^{\beta} \quad (\text{Eq. G5})$$

$$\text{Cumulative Rate:} \quad C(t) = N(t)/t = \lambda t^{(\beta-1)} \quad (\text{Eq. G6})$$

$$\text{Instantaneous Rate:} \quad c(t) = dN(t)/dt = \lambda \beta t^{(\beta-1)} \quad (\text{Eq. G7})$$

$$\text{Cumulative MTBF:} \quad M(t) = 1/C(t) = (1/\lambda) t^{(1-\beta)} \quad (\text{Eq. G8})$$

$$\text{Instantaneous MTBF:} \quad m(t) = 1/c(t) = (1/\lambda\beta) t^{(1-\beta)} \quad (\text{Eq. G9})$$

G.2.2 Reliability Growth Analysis versus Weibull Analysis

Reliability growth and Weibull analyses are both methods used to assess a product's reliability, but each has a unique purpose and application. Reliability growth analysis assesses changes in overall reliability as product improvements are made. Weibull analysis assesses the reliability characteristics of a fixed product configuration. Both analyses use time as the x-axis variable. However, for reliability growth, the x-axis variable is cumulative time (on all tested or fielded products) while for Weibull analysis, the x-axis variable is test time or service time on an individual unit. The y-axis of a reliability growth plot is failure count, failure rate, or mean time between failure. On a Weibull chart, the y-axis is probability of failure. Weibull analysis is most often used at the component level, i.e., for a specific component failure mode. In contrast, reliability growth analysis models the entire system, so that an aggregate of failure modes is included. Table G1 summarizes the characteristics of each analysis.

Table G1 - Reliability growth analysis and Weibull analysis characteristics

Reliability Growth Analysis	Weibull Analysis
1. Cumulative failures, all failure modes.	1. Individual failures for a specific failure mode.
2. Cumulative population time.	2. Individual times on failed and non-failed items.
3. Reliability is changing via product improvements.	3. Statistical characterization of a fixed product configuration.

G.2.3 Change of Slope and Goodness of Fit

An advantage of using a CROW-AMSAA plot of failures versus time is the ability to notice when changes in slope occur. This can be due to a significant design or operating change, or enough smaller design/operating changes that cause an obviously different failure rate for the system. (Example below.)

To ensure the change in failure rate is not due to natural variation, confidence bands are used to test for significance. A confidence level of 80% is typically used to provide early warning of rate changes (shown below in dashed lines). For example Figure G3 shows a typical Crow-AMSAA plot with 80% confidence bands. As you can see, the data points after 300 hours is outside the confidence band, indicating a significant change in failure rates.

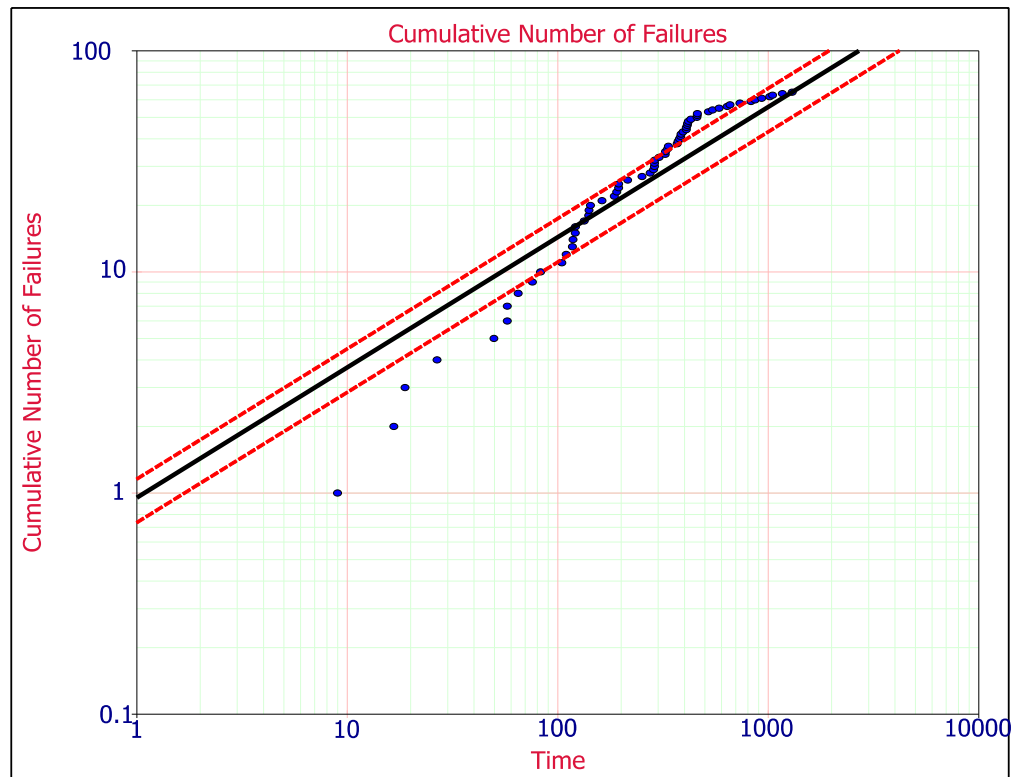


Figure G3 - Typical Crow-AMSAA chart showing 80% confidence bounds

In this case by parsing the data at 460 cumulative hours, you can see there is an improvement that occurred at over the last 1000 hours that dramatically improves the growth rate from a **constant value** to just under 0.77 (Figure G4). This is more obvious if an MTBF plot is made from the data as shown below (Figure G5).

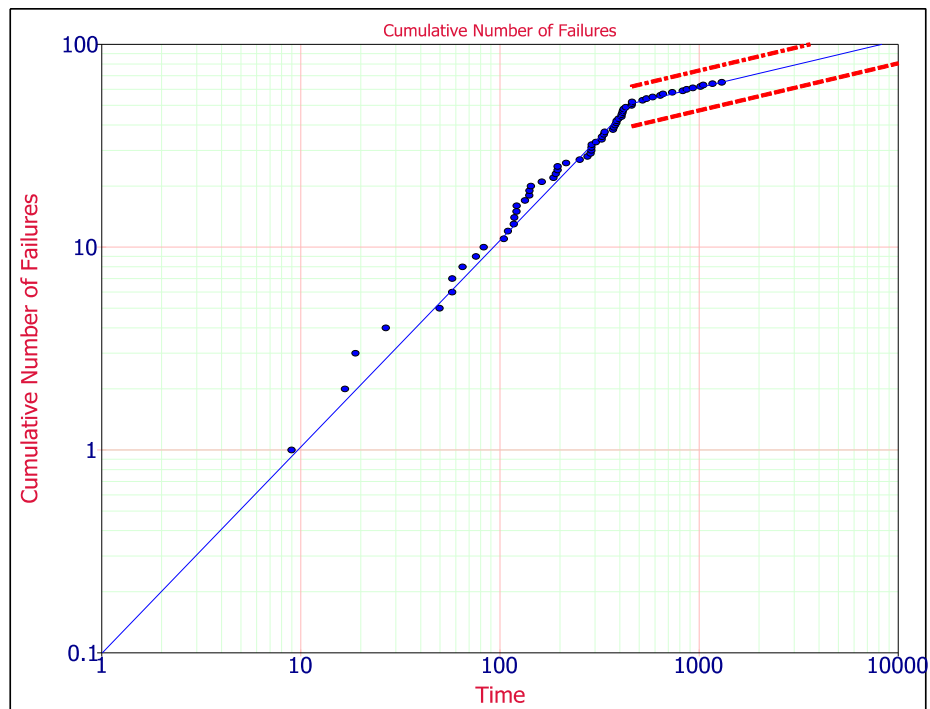


Figure G4 - Same plot with change of slope at 460 hours

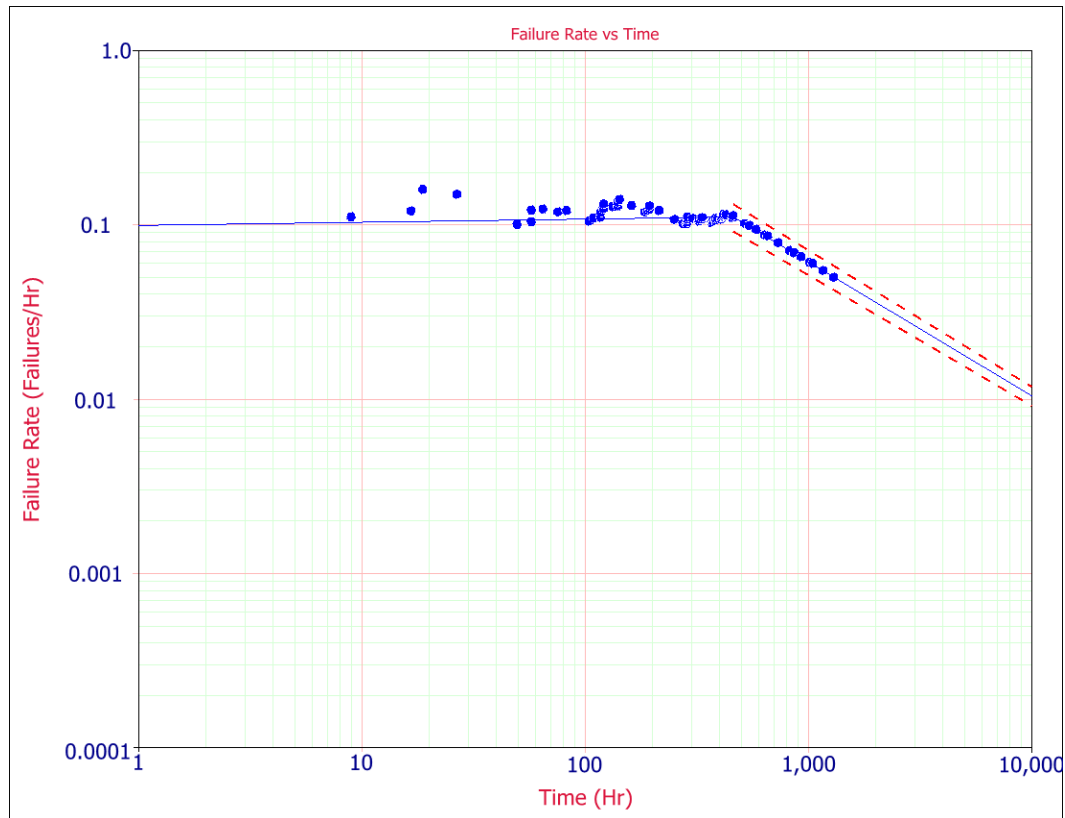


Figure G5 - Same plot showing changes in failure rate

G.3 RELIABILITY GROWTH EXAMPLE

A new product is being developed. To effectively market this product, the rate at which the product fails must be once every 1200 hours or less. In testing of the product to date, failures have occurred at 30 hours, 600 hours, 1400 hours, and 2500 hours, as summarized in Table G2.

The question to be answered is: "How much more testing (and fixing) is required to meet the failure rate desired for this product?"

To determine when the product will achieve its desired failure rate, the instantaneous (not cumulative) failure rate needs to be calculated.

Table G2 - Example testing data

Cumulative Events	Cumulative Time (hours)
1	30
2	600
3	1400
4	2500

This results in the Cumulative Events to Time plot shown in Figure G6 and Instantaneous Failure Rate to Time plot shown in Figure G7.

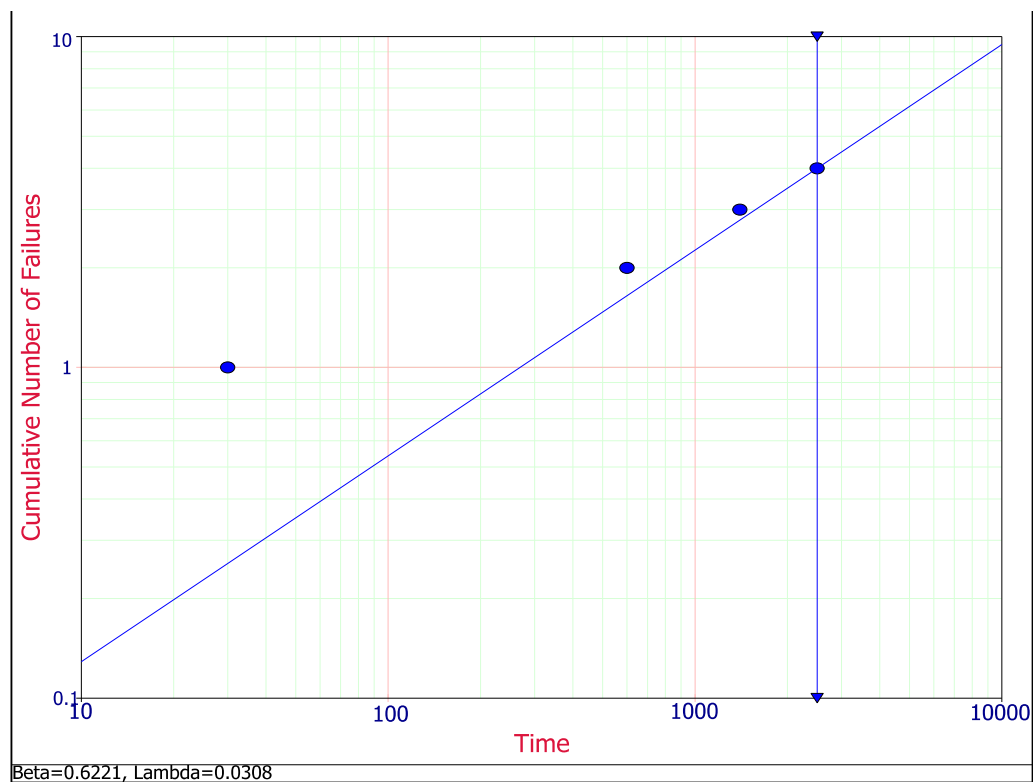


Figure G6 - Growth slope characterizations

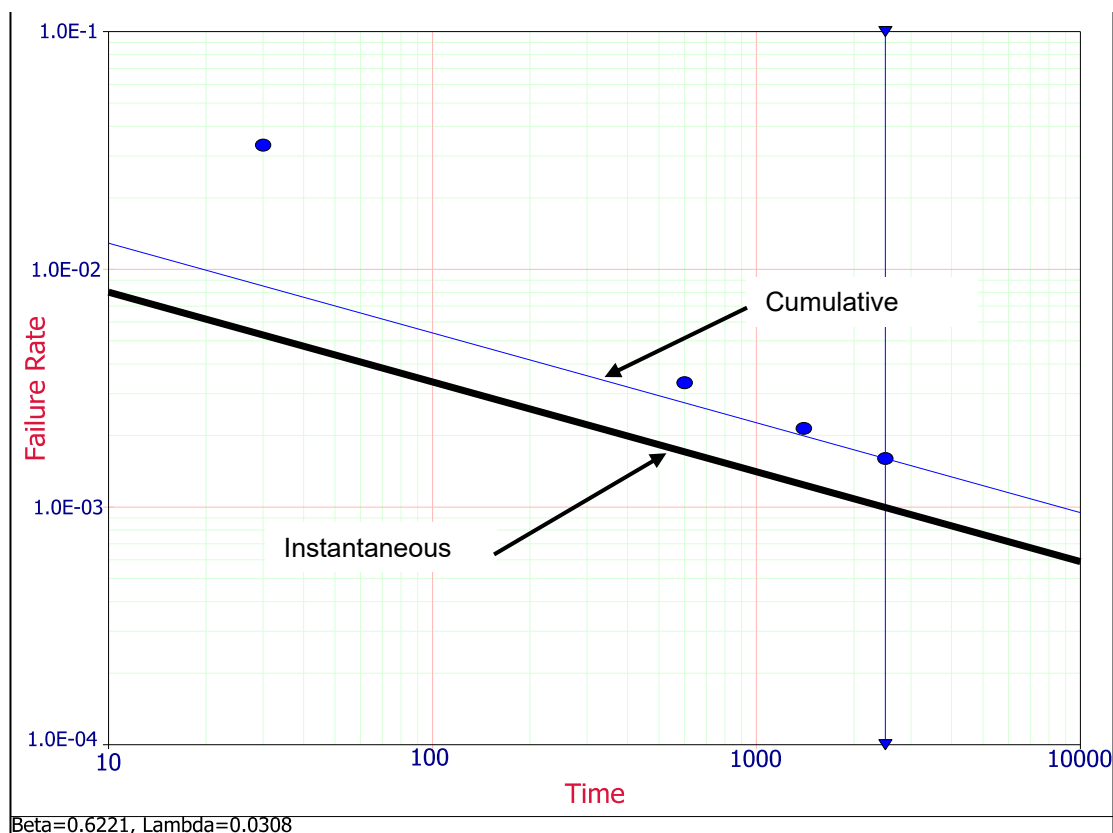


Figure G7 - Instantaneous failure rates

Plotting the data and using a Crow-AMSAA model, the predicted cumulative lambda and beta are calculated to be 0.0308 and 0.622, respectively. Using these values to model the predicted number of events and failure rate versus time you can predict when the instantaneous failure rate will drop below 0.00083 (1 in 1200):

Table G3 - Crow-AMSAA predictions

Events	Hours	Predicted Cumulative	Predicted Cumulative Rate	Predicted Instantaneous Rate	Predicted Instantaneous MTBF
1	30	0.26	0.0085	0.00530	189
2	600	1.65	0.0027	0.00170	588
3	1400	2.79	0.0020	0.00120	833
4	2500	4.00	0.0016	0.00100	1000
	3000	4.48	0.0015	0.00090	1111
	4000	5.36	0.0013	0.00083	1200
	5000	6.16	0.0012	0.00077	1305
	6000	6.90	0.0011	0.00071	1399

Based on the Crow-AMSAA plot, to achieve the 1/1200 desired failure rate an additional minimum of 1500 hours (to 4000 hours total) of testing is required, and an additional failure can be expected during this time.

The growth rate is governed by the amount of control, rigor, and efficiency by which failures are discovered, analyzed, and corrected. Growth rate values may be categorized as shown in Table G4.

Table G4 - Growth rate slope characterizations

<u>AMSAA Model</u>		<u>Comments</u>
β		Defining equations.
0.3		Maximum practical growth rate; accomplished via minimum lag time in discovering failures, analyzing them and implementing corrective actions.
<0.5		Reflects a hard hitting, aggressive reliability program with substantial management support spanning all functions.
0.5-0.7		Typical growth rate for most programs.
>0.9		Reflects growth due largely to the need to resolve obvious problems that impact production and to implement corrective actions resulting from user experience and complaints.

G.4 SUPPORTING DOCUMENTATION

In order to get in-depth understanding of the Crow-AMSAA method, it is suggested that the reader search the internet for articles on Reliability Growth, in addition to the following reference material:

- "Learning Curve Approach to Reliability Monitoring," Duane, J. T. IEEE Transactions on Aerospace, Vol. 2, No. 2, April 1964
- "Reliability Growth with Missing Data," Crow, Larry H, RAMS Proceedings, 1990
- MIL-HDBK-189C Reliability Growth Management, 2011

APPENDIX H - FLIGHT OPERATIONAL QUALITY ASSURANCE FOQA

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the body of the document.

H.1 FLIGHT OPERATIONAL QUALITY ASSURANCE PROGRAM (FOQA) - INTRODUCTION

Flight Operational Quality Assurance (FOQA) is a voluntary safety program implemented by airlines that uses de-identified, routinely recorded flight data to proactively identify and correct deficiencies in flight operations. A robust FOQA program can help the airline identify hazards and risks before they lead to an incident or accident. FOQA focuses on identifying and mitigating hazards that can exist in aircraft system design and performance, crew performance and training effectiveness, and even environmental system design. Aggregate FOQA data can be shared within the industry and with the regulators to improve the safety of the air transport industry. For example, many operators share their data under systems such as Aviation Safety Information Analysis and Sharing (ASIAS), wherein de-identified data from multiple operators help to identify systemic safety risks.

FOQA relies on an additional recording system, Quick Access Recorder (QAR), in parallel with the Digital Flight Data Recorder (DFDR). While the DFDR typically records tens of parameters, the FOQA program must consider recording routinely and continuously the hundreds, or even thousands, of parameters available on the data buses of modern aircraft. FOQA data is increasingly being used by OEM to learn more about equipment usage to help guide future system designs.

The process involves obtaining the data from the Quick Access Recorder, and then searching for and identifying flights with exceedances or special events. The data reduction software is typically capable of assigning an importance rating to the event and producing a count of the similar events. A tabulation of flights with exceedances is provided, along with an indication of the type of event and its severity. The analyst reviews the flight data recordings of these events to identify and interpret those of interest. The analyst is able to select a particular flight in the table and see the data presented in time traces for a few minutes around the event.

The identification of special events and exceedances is not the only use of flight data. On a day-to-day basis, the data provides a view of ongoing flight operations; on a longer time scale, it offers a small window into total system performance.

The concept of searching for atypical flights complements the process of searching for exceedances; i.e., the search for atypical flights may reveal unexpected phenomena and/or emerging problems that cannot be detected by the existing prescribed definitions or exceedances.

H.2 EXAMPLE LISTS OF FOQA INFORMATION

This appendix describes a list of typical FOQA parameters, termed "Triggered Events" and "Routine Operational Measurements," for use in FOQA programs. They are listed by phase of flight for transport aircraft. This is intended to be an example list and not an exhaustive checklist since it may not include all the information necessary to meet the specific operator's procedures and aircraft limitations.

Triggered Events and Routine Operational Measurements provide a method to handle the high volume of raw data collected in flight. This reduction of data limits the amount of time required to analyze the data.

The extraction of predefined parameters from raw data collected in flight provides a valuable trending and problem identification mechanism. A parameter is a measurable variable that supplies information. Typical recorded parameters are engine conditions, aircraft system characteristics (e.g., mode, status, performance limitations, flight control inputs and responses, rates of change), position information, and operating environment measurements (e.g., temperature, wind, pressure). FOQA parameters are processed into meaningful Triggered Events or Routine Operational Measurements.

H.2.1 Triggered Events

Triggered Events (TE) retain data only when the value of the specified parameter (or set of parameters) exceeds pre-defined limits set by the company and/or pilot organization. These Triggered Events may be referred to as Exceedances; however, the term is misleading in that a Triggered Event does not necessarily indicate an unsafe deviation or condition. When designing the various levels of triggers, consideration is given to compliance with federal regulations, aircraft limitations, and company policies and procedures. Multiple levels of triggers can be set. For example, within a single FOQA program, the lowest level could be set to correspond to the training and checking standards used in an Advanced Qualification Program (AQP); the next level could require higher visibility and corrective actions, while a third level might indicate when aircraft limitations were exceeded such as "flap overspeed." The Triggered Events can be valuable in identifying:

- Defective sensors on the aircraft;
- Faulty algorithms;
- Maintenance concerns such as engine over-temps, flap exceedances, or hard landings; and
- Flight operational trends that may require corrective action.

H.2.2 Routine Operational Measurements

Routine Operational Measurements are snapshots of data obtained on all flights at predefined points. Routine Operational Measurements contain only selected parameters for a moment in time. As such, they do not allow for the same in-depth analyses provided with the Triggered Event. However, since they are collected on every flight, they provide valuable trending insight into normal operations. The predefined criteria could cause data collection at a specific point in the flight (e.g., pitch attitude on takeoff, altitude for flap extension, airspeed at touchdown) or it could record an aggregate such as maximum or minimum value for the entire flight (e.g., max calibrated airspeed, minimum altitude with flaps 15, maximum bank angle below 400 feet on takeoff, maximum rate of descent, maximum pitch on landing).

Routine Operational Measurements may be categorized by the type of occurrence:

- Positional measurements which occur when the aircraft is in a specific position (e.g., 400 feet after takeoff, at the outer marker, at rotation).
- Configuration changes (e.g., position change in flaps, gear or thrust reversers).
- Aggregate, which filters out and saves the maximum, minimum or average value for the specified parameter within a defined period of time or condition (e.g., the maximum speed for flaps 5, the minimum speed below 2000 feet on approach, average fuel consumption).

H.3 FLIGHT OPERATIONAL QUALITY ASSURANCE TYPICAL EVENT CATEGORIES BY PHASE OF FLIGHT

This section describes typical items monitored, listed by phase of flight for use in FOQA programs. This is intended to be an example list, since it may not include all the information necessary to meet the specific airline procedures and aircraft limitations.

H.3.1 Taxi-Out (from Engine Start to Detection of Takeoff Thrust)

No routine operating measurements are defined for taxi-out. Some triggered events may include:

<u>Event</u>	<u>Selectable Parameters</u>
Excessive taxi speed	User-defined speed
Abnormal flight control	Position
Abnormal flap/slat/spoiler configuration	Configuration

H.3.2 Takeoff (from Detection of Takeoff Thrust to Gear Up)

Sample items that may be monitored:

- Takeoff gross weight
- Takeoff power/thrust setting
- Takeoff engine thrust set prior to throttle-hold
- Rotation occurs at appropriate speed
- Positive rate of climb prior to gear up
- Use of automation during takeoff
- Flap setting for takeoff
- Tire limit speeds not exceeded
- Engine limitations not exceeded
- Rotation on takeoff at the appropriate rate
- Altitude at gear-up
- Autothrottle targets versus actual thrust/power setting
- Pitch altitude in relation to potential tail strike

H.3.3 Initial Climb (from Gear up to 3000 feet)

Sample items that can be monitored:

- Crosswind corrections (sideslip)
- Rate of climb
- Minimum altitude for turns
- Altitude for flap retraction(s)

- Climb airspeeds
- Minimum altitude for autopilot
- Maximum airspeeds with flaps extended

H.3.4 Climb - Cruise - Descent (from 3000 Feet to First Configuration Change During Descent)

Sample items that can be monitored:

- Climb airspeeds
- Rate of climb
- Bank angle
- Maximum operating altitude
- Maximum airspeeds
- Fuel flow at stable cruise
- Navigation aid tracking
- Max altitude versus flight distance
- Flight control input versus actual control surface position
- Autopilot usage
- APU usage
- Holding pattern entry
- Winds aloft
- Bank angles
- Turbulence
- Localizer and glideslope intercept altitudes
- Airframe drag-related data
- Air-conditioning pack data

H.3.5 Approach (from First Configuration Change During a Descent to Touchdown)

There may be utility in tracking approaches. One method is to designate a minimum altitude below which the following items are monitored: engine thrust/power, rate of descent, airspeed, and aircraft configuration.

- Flap limit speeds
- Gear down speed and altitude
- Glideslope deviation at gear down
- Rate of descent at various altitudes

- Aircraft configuration
- Automation settings at various "approach gates"
- Flap extension altitudes
- Gear limit speeds
- Speedbrake limitations
- Airspeed at various altitudes
- Glideslope and localizer deviation at the outer marker, middle marker, inner marker

H.3.6 Landing (from Touchdown to Turnoff)

Sample items that can be monitored:

- Landing flaps
- Pitch attitude on landing
- Rate of deceleration
- Tire limit speeds
- Touchdown gross weight
- G-forces on landing
- Use of autobrakes
- Thrust reverser usage
- Runway tracking

H.3.7 Taxi-In (from Turnoff to Shutdown)

Sample items that can be monitored:

- Oil consumption/hour
- Fuel consumption

H.4 FLIGHT OPERATIONAL DATA ANALYSES

Flight data analyses allow users to identify significant operational safety risk areas, adopt preventive strategies, and target appropriate resources for continuous operational safety improvement. Flight data analyses include the assessment of Triggered Events, Event Trends, and Routine Operational Measurements.

H.4.1 Triggered Event Analysis

The flight data collected in conjunction with a triggered event can be used to create flight traces. Typically, most ground replay and analysis systems will capture all flight data for a time interval before and after the Triggered Event. This can also be used by visual flight animation products to create a 3-D view and a facsimile of aircraft instruments during the event.

In most cases, triggered event analysis is reduced to counts that can be filtered through various parameters. For example, "Analysis shows that 30% of flights to an airport had a high rate of descent on final approach."

Operational safety risk analysis can be conducted by assessing the exceedance severity and frequency of occurrence of the Triggered Events to provide relative rankings compared to the overall contributions of all Triggered Events. Variation in exceedances over a period of time can be identified.

H.4.2 Routine Operational Measurement Analysis

Routine Operational Measurement (ROM) analysis includes calculation and display of the way parameters are distributed over numerous flights. ROM distributions can be compared; for example, across aircraft types or registration numbers. The mean and standard deviation can be calculated for each distribution. The ROM analysis is a proactive method of providing users with hard evidence to make informed decisions and then monitor the effect of those decisions. The analysis does not need an exceedance before identifying a trend.

As an example of the relationship of parameters to Triggered Events and Routine Operational Measurements, consider data collection for Pitch Rate at Takeoff:

- First, the rate of change for the parameter called "Pitch Attitude" is computed over a defined period of time after the parameter for the "air-ground switch" changes from ground to air. In this case, data from three parameters (pitch attitude, time, and air-ground sensor), or pitch rate data may be required to define a single event.
- An associated Triggered Event called "excessive pitch rate on takeoff rotation" would extract data only when the pitch rate exceeded pre-defined values.
- An associated Routine Operational Measurement called "average pitch rate at rotation" would record the average pitch rate for every takeoff.

APPENDIX I - MAINTENANCE ERROR DECISION AID (MEDA)

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

I.1 SCOPE

The Maintenance Error Decision Aid (MEDA) is a structured process that is used to investigate events caused by mechanic/inspector performance. It is developed and distributed by Boeing Commercial Airplanes (BCA) - Commercial Aviation Services.

Maintenance and inspection errors have had serious safety consequences for the commercial airline industry. Data for the period 1990 to 2006 suggest that maintenance and inspection errors are the primary cause of about 8% of the accidents (EASA, 2007) and are a contributing factor in approximately 20 to 30% of the accidents (IATA, 2003 to 2015). In addition, maintenance and inspection errors can have large monetary consequences to the airplane operator.

We have moved away from calling MEDA an “error” investigation process to calling it an “event” investigation process. The reason for this is that it has become increasingly clear that events caused by maintenance technician and/or inspector performance can contain both an error component as well as a component involving non-compliance with regulations, policies, processes, and/or procedures. This non-compliance will be referred to as a “violation” in the remainder of this material. Maintenance errors are not made on purpose. Violations are intentional but not random and also caused by contributing factors. Data suggests that on average there are three to four contributing factors per maintenance error. These factors include such things as hard to understand maintenance manuals, poor lighting for visual inspection, lack of spare parts and calibrated equipment to carry out a maintenance task, fatigue, and poor communication. For example, poorly written manuals can be rewritten, poor lighting can be corrected, and calibrated equipment can be purchased. It is estimated that 80 to 90% of the contributing factors to error/violation are under management control, while the remaining 10 to 20% are under the control of the maintenance technician or inspector. For example, a manager may not be aware that a mechanic is concerned about a personal problem and thus might make an error during a maintenance task because of loss of concentration. Therefore, management can make changes to reduce or eliminate most contributing factors to an error or violation and thereby reduce the probability of future, similar events.

MEDA is used to investigate maintenance errors/violations that cause an unwanted outcome. It is a reactive process. MEDA can be used to investigate seven types of events:

1. Operations Process Event. (e.g., Flight delays, flight cancellations, gate returns, in-flight shut down, air turn-backs, diversion, diversion, and smoke/fumes/odor event.)
2. Aircraft Damage Event. (e.g., Airplane, ground support equipment, or vehicle damage.)
3. Personal Injury Event.
4. Rework. (Having to do a task over again because it does not pass an inspection or functional test.)
5. Airworthiness Control. (Sometimes the maintenance organization finds that something had been done incorrectly that made the aircraft unairworthy, typically after a flight with that aircraft had taken place.)
6. Found During Maintenance. (A situation where a mechanic, during a maintenance task, notices that a previously completed maintenance task had not been done correctly and needs to be rectified.)
7. Found During Flight. (A situation that pilots identifies a non-functioning system or a missing piece of equipment during flight; however, they were able to keep flying to their final destination and did not need to do an air turn back or diversion. Instead, they just make a log book entry about the system, so that the mechanics can fix the problem after the flight.)

MEDA can be used to investigate maintenance/inspection errors from any part of the maintenance organization (e.g., line maintenance, scheduled maintenance, component maintenance, engine maintenance).

The main purpose of MEDA process is not to penalize the person who commits an error or a violation, but to eliminate the underlying cause(s) for the error or violation. There is a general benefit to grant relief from punitive action to those who disclose errors/violations and thereby improve safety.

Appendix J includes details of the MEDA Process, excerpt of a MEDA User's Guide, and MEDA Results Form to document the investigations made by the airlines for this process.

Contact MHF@boeing.com for a complete MEDA User's Guide and future revisions of MEDA Results Form and User's Guide.

EXCERPT FROM
THE MAINTENANCE ERROR DECISION AID (MEDA) USER'S GUIDE

INTRODUCTION

There are three objectives of the User's Guide:

1. To give the user an overview of the MEDA philosophy and process.
2. To provide information on how to complete the MEDA Results Form.
3. To give the user examples of contributing factors to look for during the investigations.

This guide assumes that the user has been through the MEDA investigator workshop and understands the following:

- The definitions of an error and a violation.
- The definition of a maintenance system failure.
- The definition of a contributing factor.
- How MEDA provides a structured framework for investigating and documenting contributing factors to maintenance system failures and for recommending prevention strategies.

MEDA Philosophy

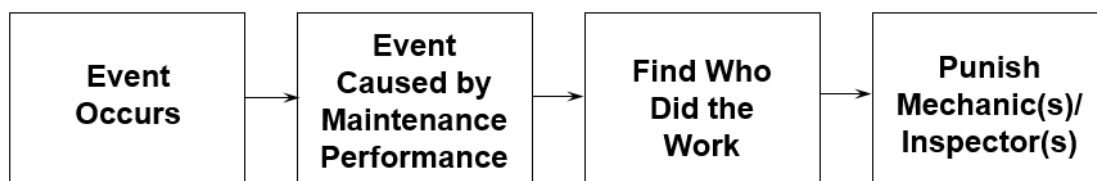
The fundamental philosophy behind MEDA is:

- Maintenance errors are not made on purpose. Errors result from a series of contributing factors in the workplace.
- Violations, while intentional, are also caused by contributing factors.
- Most of the contributing factors to errors and/or violations are under management control. Therefore, improvements can be made so that these contributing factors do not contribute to future events. Addressing lower level events helps to prevent more serious events.
- The maintenance organization must be viewed as a system, where the mechanic/inspector is one part of the system.

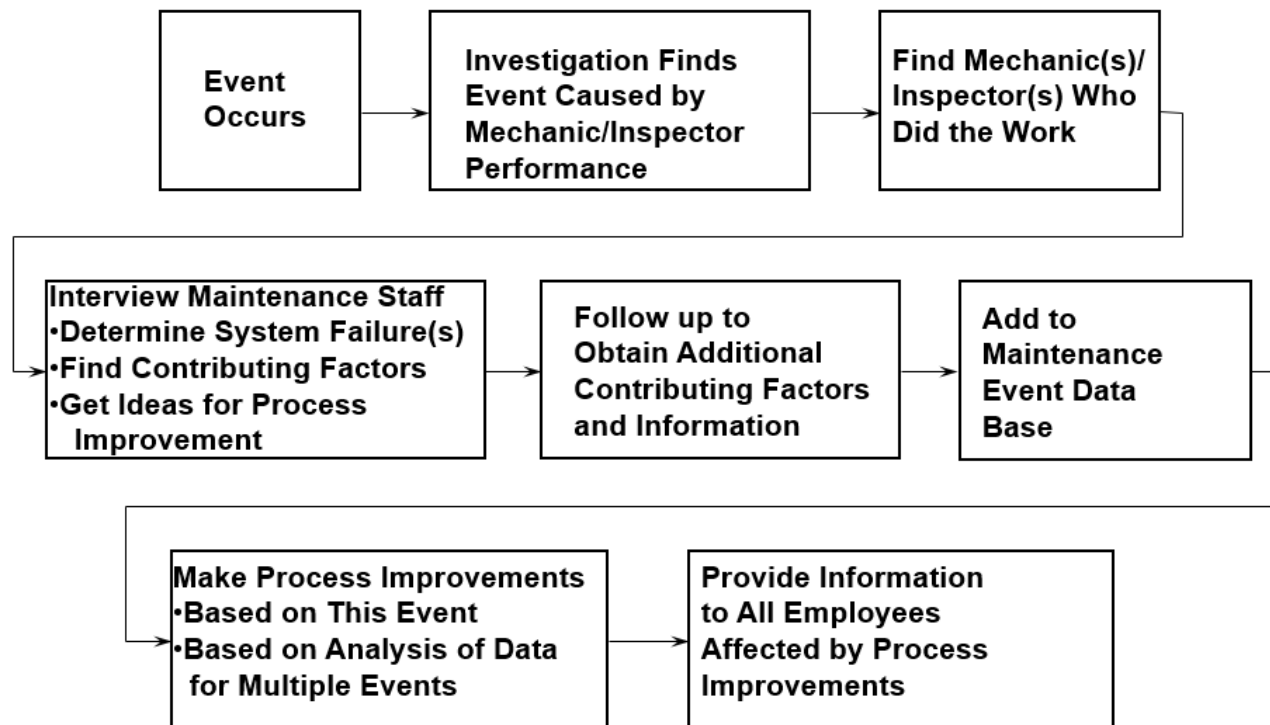
MEDA Process

MEDA is a structured process that helps airline maintenance organizations reduce maintenance events by giving them a tool to identify factors that contribute to the errors and/or violations that have led to the events. The following is a comparison of how the MEDA process is different from many traditional event investigation processes:

Traditional Event Investigation Process



The MEDA Process



INSTRUCTIONS

Use the MEDA Results Form to collect data associated with a maintenance event. Each section of the form, as shown in Figure 1, captures specific data. The end product will contain information about what happened (the event), how it happened (maintenance system failure), and why it happened (contributing factors), and recommendations to correct the contributing factors to prevent the event from occurring again. What follows are detailed instructions on how to fill in each section.

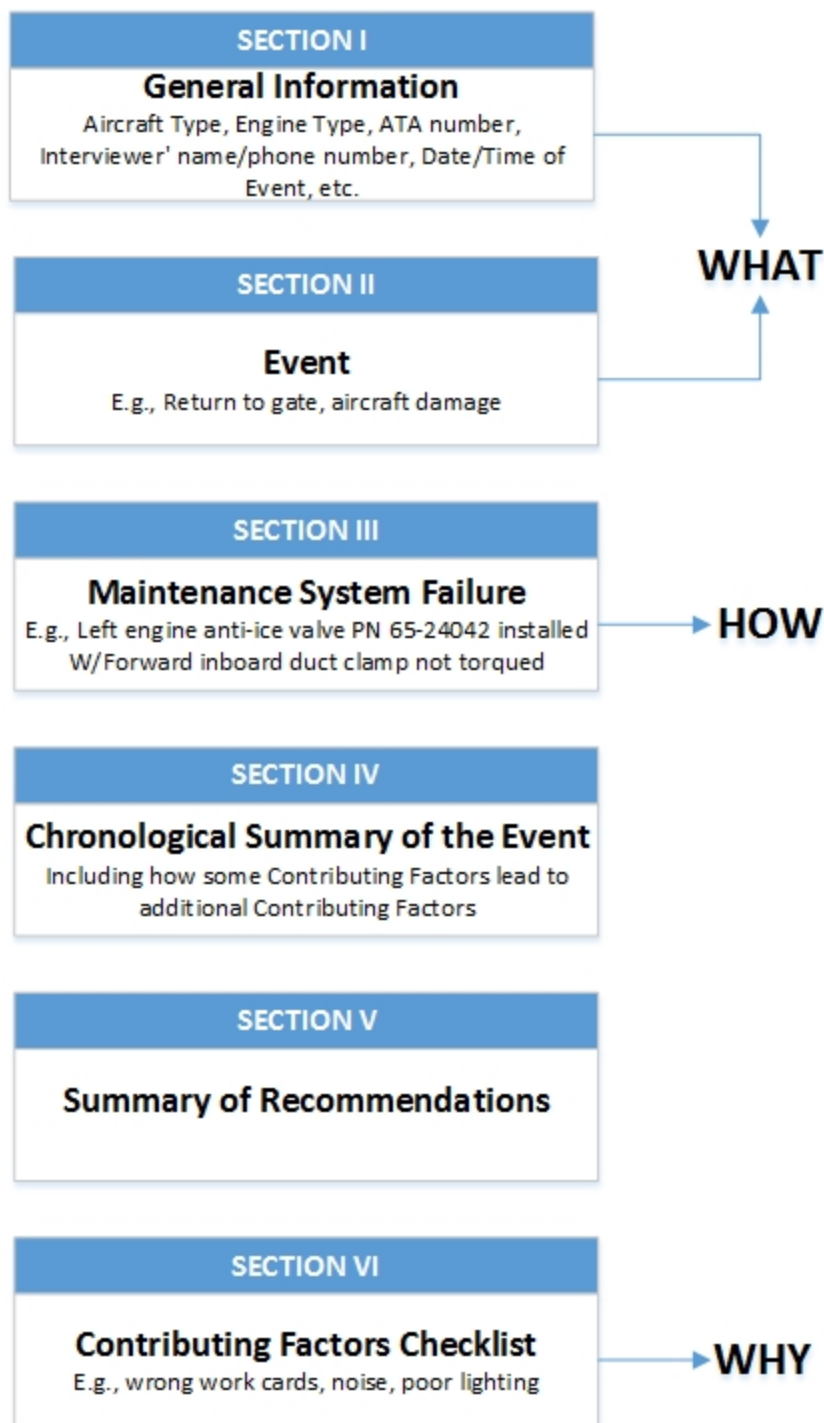


Figure 1 - MEDA Results Form Flow Chart

SECTION I - General Information**REFERENCE #**

Two letter airline designator plus three sequential numbers (e.g., BA001, BA002, etc.)

AIRLINE

Two or three letter airline designator

STATION OF MAINTENANCE SYSTEM FAILURE

Station where the Maintenance System Failure occurred NOT where it is being reported (if different)

AIRPLANE TYPE

Manufacturer and model (e.g., B747-400, DC10-30, L1011-100, A320-200)

ENGINE TYPE

Manufacturer and model (e.g., PW4000, RB211-524, CF6-80A, etc.)

REG. NUMBER

Airplane registration number

FLEET NUMBER

Letter or number designator

ATA NUMBER

Can be used to collect the ATA chapter (e.g., 30-10) most closely related to the error under investigation or the specific task card number for the task that resulted in the maintenance system failure

AIRCRAFT ZONE

e.g., 210, 130, etc.

REF NUMBER OF PREVIOUS/RELATED EVENT

If this investigation is a repeat of a similar event, use this field to reference to the previous investigation's data

INTERVIEWER'S NAME/INTERVIEWER'S TELEPHONE #

This information is required in case the someone in the organization needs clarification or more detailed information about the causes of the event

DATE OF INVESTIGATION

Date the investigation interview took place

DATE OF EVENT

Date the event occurred

TIME OF EVENT

Time of the event, if known

SHIFT OF FAILURE

Shift during which the maintenance system failure occurred, if known

TYPE OF MAINTENANCE

Indicate whether the error occurred during line or base maintenance, and what type of check or maintenance was being performed (e.g., turnaround, A-Check, overhaul, etc.)

DATE CHANGES IMPLEMENTED

Date that recommended and approved prevention strategies were implemented and documented

SECTION II - EVENT

An event is an unexpected, unintended, or undesirable occurrence that interrupts normal operations. It is entirely possible that there is more than one event checked on the form. For example, oil loss may cause an in-flight engine shutdown that is followed by a diversion.

STEP 1

CHECK AS MANY OF THE EVENT IDENTIFIERS THAT APPLY:

A. PLEASE CHECK THE EVENT

- | | |
|--|--|
| 1. Operations Process Event | ☐ 2. Aircraft Damage Event |
| ☐ a. Flight Delay __ days __ hrs. __ min. | ☐ 3. Personal Injury Event |
| ☐ b. Flight Cancellation | ☐ 4. Rework (didn't pass Ops check/inspection) |
| ☐ c. Gate Return | ☐ 5. Airworthiness Control |
| ☐ d. In-Flight Shut Down | ☐ 6. Found during Maintenance |
| ☐ e. Air Turn-back | ☐ 7. Found during Flight |
| ☐ f. Diversion | ☐ 8. Other Event (explain below) |
| ☐ g. Smoke/fumes/odor event | |
| ☐ h. Other (explain below) | |

STEP 2

DESCRIBE THE INCIDENT/DEGRADATION/FAILURE (E.G., COULD NOT PRESSURIZE) THAT CAUSED THE EVENT.

It is important that you not just check the box to indicate which event(s) occurred. You should write additional information in the blank space in the block.

Example: During take-off, an off-wing escape slide inadvertently deployed hitting and damaging the side and the tail of the airplane.

SECTION III - MAINTENANCE SYSTEM FAILURE

A maintenance system failure (whether it is caused by an error, a violation, or an error/violation combination) leads directly to the event. The system failures that are listed are very specific and relate easily to maintenance technician and inspector performance. There are eight different major system failures:

1. Installation failure
2. Servicing failure
3. Repair failure
4. Fault isolation, test, or inspection failure
5. Foreign object damage/debris
6. Airplane or equipment damage
7. Personal injury
8. Maintenance control failure.

A ninth box is provided for "Other" in case the specific system failure of interest was not listed in 1 to 8 above.

STEP 1

SELECT THE TYPE OF MAINTENANCE SYSTEM FAILURE BY PUTTING A CHECK MARK (✓) IN THE CORRECT BOX OR BOXES.

NOTE: Sometimes several system failures combine to cause an event. It is important to keep track of which prevention strategies and contributing factors listed in Sections V and VI relate to which system failures identified in Section III. This could be done in several ways. For example, you could fill out one Results Form for each system failure. Alternatively, you could check one system failure box with a red pencil and the second with a blue pencil. Then the factors that contributed to the first system failure could be written in red and the factors that contributed to the second system failure could be written in blue. Or, you could put a * by the first system failure and a # by the second system failure. Then you could place a * by the factors that contributed to the first system failure and a # by the factors that contributed to the second system failure.

STEP 2

ANSWER THE QUESTION, “DID THE MAINTENANCE SYSTEM FAILURE “FLY” ON THE AIRCRAFT?”

Check “Yes” if the system failure was not caught before the next flight of the aircraft. Check “No” if the system failure was found and corrected before the next flight of the aircraft.

STEP 3

WRITE A BRIEF WRITTEN DESCRIPTION OF THE MAINTENANCE SYSTEM FAILURE IN THE OPEN SPACE BELOW THE LISTED SYSTEM FAILURES.

Example: It appears the maintenance technician failed to secure the escape slide carrier pin and one or both door latches.

SECTION IV - CHRONOLOGICAL SUMMARY OF THE EVENT

The purpose of this section is to describe and summarize the event in a chronological order and what an investigator found regarding contributing factors during the interview. If any of the identified contributing factors lead to additional contribution factors, make sure those causal relationships are documented here as well.

SECTION V - SUMMARY OF RECOMMENDATIONS

It is recommended that each or a combination of identified contributing factors is summarized in the following manner: First of all, write down a “Recommendation #” (e.g., 1, 2, 3, etc.), so that it is easier to refer to later on. For each recommendation, record the corresponding “Contributing Factor #” (e.g., A.1. for Information Not Understandable). [Note: One Recommendation might be related to two or more contributing factors.] Third, write down the proposed improvement to be made to the contributing factor(s) that you listed (e.g., rewrite the third step in the engineering order to make clear what the torque values are supposed to be).

SECTION IV - CONTRIBUTING FACTORS CHECKLIST

This checklist will help the analyst identify the contributing factors that contributed to the maintenance system failure. If several maintenance system failures combined to cause the event, it is important to remember to identify and document only those factors contributing to one failure at a time.

STEP 1

Check all the applicable contributing factors for the error identified in Section III. See the Contributing Factors Checklist Examples section for additional information on each factor.

STEP 2

If a contributing factor on the list was not involved, check N/A. The purpose of this step is to ensure that each contributing factor is considered during the investigation and analysis.

STEP 3

For each factor identified, give a written description of how it contributed to the maintenance system failure.

HOW TO CARRY OUT THE MEDA INVESTIGATION INTERVIEW

It cannot be emphasized enough that the most important part of the investigation is the interview with the maintenance technician/inspector, whose performance lead to the event, in order to find out the contributing factors to the error and/or violation. Interviewing is a skill just like using a torque wrench is a skill. You will get better at interviewing the more interviews that you carry out. There are three purposes of this section:

1. To discuss who should be on the interview team,
2. To provide guidelines for how to carry out the interview, and
3. To provide some specific rules of causation.

The MEDA Interview Team

How many people should be on the interview team? The advantage of one person doing the interview is that one person is typically less threatening to the technician than several people. However, this person must be a good interviewer, since he/she has to do all of the work himself/herself. You may find that you start off with a 2-person interview team, but as the interviewers gain experience, you can move to a smaller team.

The advantage of a 2-person team is that one person can be asking questions while the second person is writing down information. In addition, the second person may think of additional questions to ask. When an organization first implements MEDA, they often start with a 2-person interview team.

We typically suggest that 3 people are too many on the interview team. The technician could start to feel outnumbered, and, therefore, uncomfortable and unwilling to tell everything that he/she knows. However, a 2-person team with a union observer has proven useful at unionized maintenance organizations. The union observer's job is to let the maintenance technician know that the union supports the MEDA process and to encourage the maintenance technician to cooperate during the interview.

Who should be on the interview team? First, whoever is on the team should have some form of MEDA training. Hopefully, that is training provided by Boeing, but it could be training provided by your training organization. Even if you receive the Boeing MEDA Investigator Workshop training, additional training on interviewing is helpful, especially if the training includes practice at interviewing that is possibly videotaped for audio and visual feedback.

Guidelines for the MEDA Investigation Interview

Once the team has been chosen, it is time to carry out the MEDA investigation interview. MEDA uses a method of interviewing called "Cognitive Interviewing." The Cognitive Interview technique is a systematic information retrieval strategy that has been shown to increase the amount of information that is recalled. More specifically, it typically elicits 30 to 70% more correct information than conventional interviewing procedures (e.g., police accepted practice), and leads to an equivalent or slightly higher accuracy level (proportion of statements that are accurate) when compared to conventional interviewing procedures.

Cognitive Interviewing is based on a method for interviewing witnesses of criminal events (Fisher & Geiselman, 1992). It is a systematic approach to interviewing cooperative interviewees based on scientific principles of memory and communication. The principles of cognition are converted into a number of specific techniques to help interviewees improve their memory performance, including:

- Encouraging the interviewee to concentrate
- Recreating the event context
- Explicitly requesting detailed descriptions
- Focusing on obtaining as much information as possible about a topic before moving on to another topic.

Cognitive Interviewing is consistent with the guidelines provided in other sources. There are some general principles of investigate interviewing that should be followed throughout all stages of the interview. These include:

- Develop and maintain good rapport.
- Encourage the interviewee to be actively involved.
- Help the interviewee concentrate.
- Use open, simple, and unbiased questions.
- Listen actively.
- Use a communication style to suit the interviewee.
- Work as a team with other interviewers.

There are specific stages of the interview that should be followed. These stages include:

1. Pre-Interview Preparation and Planning
2. Interview
 - a. Introduction
 - b. General Account of Event/Task
 - c. Detailed Account of Parts of the Event/Task
 - d. Background Information
 - e. Conclusion
3. Post-Interview Evaluation and Follow-up

RULES OF CAUSATION

Filling out the MEDA Results Form correctly, so that the collected information provides maximum value to the organization, is not an easy task. We have found that if the interviewer keeps six “rules of causation” in mind, then the task can be made easier.

Rule 1 — Each human error must have a preceding contributing cause.

The investigation must search beyond the error to why the error has occurred. Most mishap investigations tend to stop at the mere identification of the human error. However, we need find out the contributing factors that led to the human error in order to find the best way to correct the error. Some common human errors include:

- Failure to properly document maintenance in maintenance records, work package
- Inattention to detail/complacency
- Incorrectly installed hardware on an aircraft/engine.

Rule 2 — Each procedural deviation (violation) must have a preceding cause.

Procedural deviations (violations) are a common contributing factor to error. However, in order to determine the best way to “fix” the procedural deviations, we need to know why the deviation occurred. Therefore, it is important, when you determine during the interview that a procedural deviation occurred, to find out why the technician deviated. Some common procedural deviations include:

- Failure to use the maintenance manual/task card
- Failure to use torque wrench or other calibrated equipment
- Failure to carry out a functional or operational check at the end of a procedure

In each of these cases, it is important to find out why the technician decided to deviate from the accepted procedure.

Rule 3 — Causal statements must clearly show the “cause and effect” relationship.

The relationship between the contributing factor and the error and/or violation must be clearly written down. This is one of the most important rules for filling out the MEDA Results Form. You must write in the appropriate contributing factors section how the contributing factors that you checked actually contributed to the error and/or the violation.

Rule 4 — Negative descriptors, such as “poorly” or “inadequate,” may not be used.

If you just say that something was done “poorly” or “in an inadequate fashion,” it is not clear what the corrective action is. Saying that the maintenance manual was written “poorly” does not tell someone how to rewrite the manual. We must be specific about what the real issue is. For example, “The maintenance technician was working in the vertical tail fin of the aircraft, and the task required that he/she face towards the rear of the aircraft. The maintenance manual tells him to “loosen the left bolt” (of two bolts side by side). The technician loosened the bolt on his left, but the maintenance manual was actually referring to “aircraft left.”

Rule 5 — Failure to act is only causal when there is a pre-existing duty to act.

This is an important rule of causation that comes from legal findings. We should not expect someone to do something unless there is a pre-existing duty to do that thing. For example, we do not expect you to start leaving home for work 30 minutes earlier than usual just in case there is an unexpected traffic problem. We do not expect an inspector to do a full entry fuel tank inspection when the task only calls for an inspection that has the inspector putting his head through the access and using a flashlight and a stick with a mirror to do the inspection. We do not expect a technician to carry out a functional task twice just in case the first test was not enough. It is important to know in these situations exactly what pre-existing duties technicians/inspectors have. For example:

- Before closing an access panel, does the technician have a clearly stated duty to do a visual inspection of the area before closing the panel?
- If the technician is not sure how to proceed on a task, does he have a clearly stated duty to get help from the lead/supervisor/engineer before proceeding?
- If the technician deviates from a procedure, does he have a clearly stated duty to document the deviation?

Rule 6 — Causal searches must look beyond that which is within the control of the investigator.

If the investigators are not in a position to change the contributing factor, they have the tendency to stop the investigation at factors only within their control. There is a belief that there is no reason to identify as causal what you cannot change. However, what might not be changeable from a single investigation might in fact be changeable if it is present in an entire class of events. Thus investigative conclusions should not be controlled by the investigator's perceived extent of control.

CONTRIBUTING FACTORS CHECKLIST

EXAMPLES

A. Information

Information refers to the written or computerized source data that a maintenance technician or inspectors needs to carry out a task or job. It includes work cards or task cards, maintenance manual procedures, service bulletins or engineering orders, maintenance tips, illustrated parts catalogs and other manufacturer supplied or internal resources. Information does not include verbal instructions from supervisors, shift handover logs, etc., which are considered to be Communication on the Results Form

To determine that information was a contributing factor to the maintenance system failure, either the information itself must be problematical (e.g., hard to understand, not complete, conflicting), or the information should have been used but was not (e.g., it was not available, it was not used). If it is expected that the maintenance technician has this information memorized, then refer to the Technical Knowledge/Skills section.

Examples to look for:

1. *Not understandable*

- Unfamiliar words or acronyms
- Unusual or non-standard format
- Poor or insufficient illustrations
- Not enough detail or missing steps
- Poorly written procedures

2. *Unavailable/inaccessible*

- Procedure does not exist
- Not located in correct or usual place
- Not located near worksite

3. *Incorrect*

- Missing pages or revisions
- Does not match aircraft configuration
- Transferred from source document incorrectly
- Steps out of sequence
- Not the most current revision
- Procedure does not work

4. *Too much/conflicting information*

- Similar procedures in different resources do not agree (e.g., aircraft maintenance manual [AMM] versus task card)
- Too many references to other documents
- Configurations shown in different resources do not agree

5. *Update process is too long/complicated*

- Requested revisions have not been incorporated yet
- Configurations changed by Service Bulletins (SB) or Engineering Orders have not been updated in applicable maintenance procedures
- Document change requests are not submitted, lost, or incorrectly filled out

6. *Incorrectly modified manufacturer's MM/SB*

- Intent of manufacturer's procedure is not met
- Non-standard practices or steps are added
- Format does not match rest of procedure or other procedures

7. *Information not used*

- Not using technical documentation is potentially a violation. If the technician should have used the documentation, but did not, find out why (i.e., what the contributing factors were to not using the documentation).
- Procedure available but the technician did not have enough time to get it
- Technician thought that he/she did not need the procedure because he/she had done the task many times before

8. Inadequate

- The technical documentation did not include a detailed enough task level description for the technician to carry out the task correctly.
- The technical documentation did not include technical information needed to carry out the task, e.g., torque values or loop resistance values.
- The technical documentation did not include enough figures or graphics to help explain clearly what needed to be done by the technician.

9. Uncontrolled

- The technician used an uncontrolled copy of technical documentation, and the differences between the uncontrolled documentation and the controlled documentation contributed to the error.
- Technician used his/her "black book," and the information was no longer correct.

10. Other

- Operator cannot use digital information

B. Ground Support Equipment, Tools, and Safety Equipment

Ground support equipment/tools/safety equipment are the tools and materials necessary for the safe performance of a maintenance task. Equipment and tools refer to things such as work stands, calibrated torque wrenches, screwdrivers, test boxes, and special tools called out in maintenance procedures. Safety equipment includes both personal protective equipment, such as hearing protection, toe protection, and safety harnesses, as well as collective safety devices, such as hazard barriers and safety railings.

Unsafe equipment and tools may cause a maintenance technician or inspector to become distracted from the task due to concern for personal safety. If equipment or tools are not available or are inaccessible, the maintenance technician or inspector may use other equipment or tools that are not fully suited for the job. Other factors that can contribute to system failure include out of calibration instruments, use of unreliable equipment, or equipment or tools with no instructions for use.

Examples to look for:

1. Unsafe

- Platform moves and is unstable
- Brakes or safety devices inoperative
- Non-skid material worn or missing
- A lock-out mechanism is missing or faulty
- Placards (warnings or cautions) are missing or faded
- Sharp edges are exposed or personal protective devices are missing
- Power sources are not labeled or protected

2. Unreliable

- Intermittent or fluctuating readings on dials or indicators
- Damaged or worn out
- Expired use limits
- History of defects

3. Layout of controls or displays

- Easy to read wrong display or use wrong control
- Awkward locations, hard to reach
- Too small to read or control
- Directional control of knobs or dials is not clear

4. Out of calibration

- Tool out of calibration from the start of use
- Wrong specifications used during calibration procedure

5. Unavailable

- Is not owned or in stock
- Not available for procurement

6. *Inappropriate for the task*

- Standard hand tools used for leverage
- Not capable of handling weights, forces, or pressures required for the task
- Connections or grips not the right size

7. *Cannot use in intended environment*

- Not enough space to operate tool
- Requires level surface where one is not available

8. *No instructions*

- Instructional placards missing or faded
- Directional markings missing
- Tool usage instructions not available

9. *Too complicated*

- Tool usage requires too many simultaneous movements and/or readings
- Fault isolation or testing is too complex

10. *Incorrectly labeled*

- Hand marked labeling or operating instructions are incorrect
- Tool has incorrect scale readings

11. *Not used*

- Equipment/tool/part is available but not used. Not using the correct equipment/tools/safety equipment is potentially a violation. If the technician or inspector did not use the correct equipment/tools/safety equipment, find out why (i.e., what the contributing factors to not using it).

12. *Incorrectly used*

- Safety equipment not appropriate for the hazard
- Personal protective equipment not properly worn

13. *Inaccessible*

- Not in usual location (possibly being used on other task or aircraft)
- Too far away from the worksite

14. *Past expiration date*

- The valid calibration date for torque wrench has expired.

15. *Other*

- System protection devices on tools/equipment not available

C. Aircraft Design, Configuration, Parts, Equipment, and Consumables

An aircraft should be designed/configured so that parts and systems are accessible for maintenance. Equipment and consumables need to be available and accessible. The maintenance technician should be able to see and reach a part, should be able to remove it from a reach and strength standpoint, and should be able to easily replace the part in the correct orientation. When reviewing accessibility as a contributor to maintenance system failure, it must be seen as a real contributor to the system failure and not just as an inconvenience to the maintenance technician or inspector.

Configuration variability between models and aircraft can contribute to system failure when there are small differences between the configurations that require maintenance tasks to be carried out differently or require slightly different parts.

Parts refer to aircraft parts that are to be replaced. Equipment refers to required equipment per a maintenance or inspection procedure. Consumables refer to materials (e.g., grease, fluorescent dye) that to be consumed for a specific maintenance or inspection task or job. Incorrectly labeled parts can contribute to improper installation or repair. Parts or equipment or consumables that are unavailable or expired can contribute to system failure by the maintenance technician/inspector who substitute or skip the required part or equipment or consumables.

Good part design also incorporates feedback that helps the maintenance technician know that something has been performed correctly. For example, an electrical connector that has a ratchet effect provides feedback to the maintenance technician when the installation is correct. If this ratchet effect is included in some connectors and not others, this could contribute to system failure. If a maintenance technician goes from a ratchet connector to a non-ratchet connector, the technician may over tighten the second connector looking for the ratchet.

Examples to look for:

1. *Complex*

- Fault isolation on the system or component is difficult
- Installation of components is confusing, long, or error prone
- Multiple similar connections exist on the system or component (electrical, hydraulic, pneumatic, etc.)
- Installation tests for the component are extensive and confusing
- Different sized fasteners can be installed in multiple locations

2. *Inaccessible*

- Components or area to be maintained is surrounded by structure
- No access doors exist in the maintenance area
- Area lacks footing space or hand-holds
- Small or odd-shaped area

3. *Aircraft configuration variability*

- Similar parts on different models are installed differently
- Aircraft modifications have changed installation or other maintenance procedures between aircraft

4. *Parts/equipment unavailable*

- Part not owned or in stock
- Not available for procurement

5. *Parts/equipment incorrectly labeled*

- Hand marked labeling incorrect
- Wrong part number on part

6. *Inappropriate for the task*

- Consumables (e.g., tapes, rags) are the same color as the inside of the fuel tanks
- Not capable of handling weights, forces, or pressures required for the task

7. *Easy to install incorrectly*

- Can be easily installed with wrong orientation
- No orientation indicators (e.g., arrow, colors)
- Connections identical in size, color or length

8. *Not used*

- Correct part was available to use, but technician did not use it and used a different (non-interchangeable) part instead
- Correct part was unavailable, so technician used a different (non-interchangeable) part
- If the correct part was available, but was not used, then this could be a violation. If the technician did not use the correct part when it was available, find out why (i.e., what the contributing factors to not using it).

9. *Not user friendly*

- Lack of feedback provided by component or system
- Can be easily installed with wrong orientation
- Direction of flow indicators do not exist.

10. *Consumable unavailable*

- High-temperature grease is unavailable

11. Wrong consumable used

- Low temperature instead of high-temperature grease was used

12. Expired consumable used

- Grease was past its pull date.

13. Other

- Components are too heavy for easy removal/installation
- Lack of feedback provided by component or system
- Direction of flow indicators do not exist

D. Job and Task

A maintenance technician's job/task can logically be separated into a series of tasks. If the interviewer feels the task was a contributing factor, he/she should analyze the combination or sequence of tasks. The interviewer, when examining the task sequencing, should also determine whether written information was being used, what technical skills and knowledge were expected of the maintenance technician, and what communication took place.

Examples to look for:

1. Repetitive/monotonous

- Similar steps are performed over and over (opening and closing circuit breakers during a long test)
- The same task performed many times in multiple locations (removing seats)
- Checking the expiration date for all of the onboard life jackets

2. Complex/confusing

- Multiple other tasks are required during this task
- Multiple steps required at the same time by different maintenance technicians
- Long procedure with critical step sequence
- System interacts with other systems during testing or fault isolation
- Multiple electrical checks are required
- Task requires exceptional mental or physical effort

3. New task or task change

- New maintenance requirement or component
- Revision to a procedure
- Engineering modification to existing fleet
- New aircraft model

4. Different from other similar tasks

- Same procedure on different models is slightly different
- Recent change to aircraft configuration has slightly changed task
- Same job at different worksites is performed slightly different

5. Other

- The workgroup performs the task differently than specified in the source data (or written information)

E. Knowledge and Skills

Technical skills refer to tasks or subtasks that maintenance technicians or inspectors are expected to perform without having to refer to other information. Technical skills include such things as being able to lock wire, use a torque wrench, remove common parts from an aircraft, and perform a general visual inspection for corrosion. For (lack of) technical skills to be a contributing factor to system failure, the technician must not have skill that was generally expected of him/her.

Technical knowledge refers to the understanding of a body of information that is applied directly to performing a task. Technical knowledge, in order to be a contributing factor to system failure, is knowledge that is supposed to be known (memorized) by the maintenance technician or inspector. Three broad categories of knowledge are required of a technician or an inspector: airline process knowledge, aircraft systems knowledge, and maintenance/inspection task knowledge. These are discussed in more detail below.

Airline process knowledge refers to knowledge of the processes and practices of the airline or repair station in which the maintenance technician or inspector works. Examples include shift handover procedures, parts tagging requirements, and sign-off requirements. While this knowledge is generally acquired through general maintenance operating procedures and on-the-job discussion with peers, it may also be acquired from other sources such as employee bulletins and special training.

Aircraft system knowledge refers to knowledge of the physical aircraft systems and equipment. Examples include location and function of hydraulic pumps and rework options for corroded or fatigued parts. While this knowledge is generally acquired from the aircraft design characteristics, training, maintenance manuals, and on-the-job discussion with peers, it may also be acquired from other sources such as trade journals and maintenance tips.

Maintenance/inspection task knowledge refers to the specific knowledge required to perform a unique task. Examples include the procedure for bleeding a hydraulic system and for measuring tire wear. While this knowledge is generally acquired through maintenance instructions or on-the-job discussions with peers, it may also be acquired from aircraft placards, design characteristics, or even other maintenance technicians when working as a team.

English language proficiency refers to a maintenance technician or inspector's ability to speak and read English.

Teamwork skills refer to an individual technician or inspector's skills with regard to working on a team. The technician or inspector may lack the skills needed just to participate on a team—e.g., active listening, questioning/assertiveness, persuading, respecting, helping others, sharing, and participating. The team may also lack the skills needed to carry out team tasks—e.g., setting clear goals, being results driven, gaining consensus, and leadership.

Computing skills refer to a technician or an inspector's skills in using a computer. This includes—e.g., finding information on a computer, generating requests (such as for non-routine tasks), and entering information into a computer (such as employee identification information, task completion information, and ETOPS oil monitoring values).

Examples to look for:

1. *Technical skills*

- Safety wiring
- Rigging of controls
- Using calibrated equipment
- Carrying out a fault isolation task
- Removing and replacing parts

2. *Task knowledge*

- Slow task completion
- Technician change of maintenance responsibilities
- Task performed by maintenance technician for the first time
- Task performed in wrong sequence

3. *Task planning*

- Frequent work interruptions to get tools or parts
- Failure to perform preparation tasks first
- Too many tasks scheduled for limited time period
- Task necessary for safety not performed first

4. *Airline process knowledge*

- If the technician knows the correct airline process to follow, but does not do so, then this could be a violation. If the technician did not follow the process correctly, find out why (i.e., what the contributing factors to not following the airline process).
- Failure to acquire parts on time
- Technician new to airline or to type of work (from line to hangar, etc.)
- Airline processes not documented or stressed in training

5. *Aircraft system knowledge*

- Technician changes aircraft types or major systems
- Fault isolation takes too much time or is incomplete

6. *English language proficiency*

- Technician made mistake because they could not read English technical documentation well enough
- Technician made mistake because they could not understand spoken English well enough

7. *Teamwork skills*

- Technicians arguing with each other about how to carry out/continue a task
- One technician ignoring another technician's input on what to do next
- One technician does not trust another technician to do what was promised.

8. *Computing skills*

- Technician cannot access technical documentation on the local intranet
- Technician cannot generate a non-routine in SAP (or other maintenance-related computing system)
- Technician does not enter Extended Operations (ETOPS) oil monitoring information into the correct database because he/she cannot access the database and/or enter the data correctly.

9. *Other*

- Technician performance/skills not accurately tracked/measured

F. Individual Factors

Individual factors vary from person to person and include body size/strength, health, and personal events and the way that a technician responds to things such as peer pressure, time constraints, and fatigue caused by the job itself.

Physical health includes the acuity of human senses as well as physical conditions and physical illnesses. Human senses, especially vision, hearing, and touch, play an important role in maintenance and inspection. Technicians and inspectors are frequently required to perform tasks that are at or near the limits of their sensory capabilities. For example, some tasks require good vision and/or touch, such as visual inspection for cracks or finger inspection for burrs. Good hearing is also required in order to hear instructions or feedback before and during a maintenance task.

Physical conditions, such as headaches and chronic pain, also have been shown to relate to system failures. Alcohol/drug use, as well as side effects of various prescription and over-the-counter medicines, can negatively affect the senses. Physical illness, such as having a cold or the flu, can also negatively affect the senses and the ability to concentrate. Illnesses can also lead to less energy, which can affect fatigue.

Fatigue has been defined by the U.S. Federal Aviation Administration (FAA) as a depletion of body energy reserves, leading to below-par performance. Fatigue may be emotional or physical in origin. Acute fatigue may be caused by emotional stress, depletion of physical energy, lack of sleep, lack of food, poor physical health, or over excitement. Fatigue may also be caused by the work situation itself. The time of the day, the length one has been working, and complex mental tasks or very physical tasks can cause fatigue.

A technician's response to time pressure is an individual factor. The need to finish a maintenance task so an aircraft can be released from the gate or to finish a heavy maintenance task so an aircraft can be put back into service often cause technicians to feel pressure to get their tasks done. Studies have linked too little time with increased error and/or likelihood to engage in situational violations. There is a well-known phenomenon called the speed/accuracy trade-off. People learn to do tasks at a certain speed, like typing or keyboarding. If you ask the person to type more quickly, they can, but they will make more errors (trading off errors for more speed). If you ask the person to make no errors while typing, they will slow down (trading off speed for fewer errors). This trade-off also holds for speed and working safely. So, anytime that you tell a technician to "hurry up and finish that task," you are increasing the probability that they will make an error.

Peer pressure is the pressure that a technician/inspector's colleagues put on him/her to conform to the way the other members of the group carry out their work. A technician's response to peer pressure can influence their performance. For example, there may be peer pressure not to use maintenance manuals because it is seen as a sign of lack of technical knowledge. Peer pressure may also influence a technician's safety-related behavior.

Complacency is over-contentment with a situation that may lead to a failure to recognize cues that indicate a potential error.

Body size and strength are two obvious factors that affect a maintenance technician's ability to perform a task. If someone is too short to reach a plug or if someone is not strong enough to let down a Line Repairable Unit (LRU) from an upper rack, this can contribute to system failure.

Personal events can affect a technician's ability to concentrate on a task. For example, if the technician had a fight with his/her spouse that morning, was in a car accident on the way to work, or has a daughter in the hospital with a life-threatening disease, the technician may start thinking about these events during task accomplishment rather than concentrating on the task itself.

Task distractions/interruptions refer to anything that causes a technician to quit working on the task at hand for any period of time. For example, a technician may be called over to help someone lift a heavy component into place or a lunch break may occur. In those cases, at least, the same technician continues to carry out the task. A very common contributing factor to an error is when task completion is interrupted by the end of the shift. In this case, the technician often has to hand over the task to someone else, so that communication issues may also play a part in an error.

Memory lapse (forgot) refers to a failure to remember something at the necessary time.

Visual perception is the ability to interpret information from visible light reaching the eye. The resulting perception is also known as eyesight, sight or vision. The various physiological components involved in vision are referred to collectively as the visual system. A technician may not visually perceive (see) something correctly for a variety of reasons, including optical illusions, parallax, inadequate lighting, obstructed view, and being too close or too far away from the object of interest.

Assertiveness is being willing to speak your mind and to state and maintain your individual position on an issue.

Stress is your body's physiological reaction to physical and psychological factors (stressors) in your environment. Stress can cause emotional, muscular, digestive system, and other physical symptoms (e.g., high blood pressure, increased heart rate, migraine headaches, and dizziness). Any of these things can interfere with a technician's ability to concentrate on task accomplishment.

Situation awareness is a technician's ability to maintain awareness of what is happening on the ramp or the hangar, as well as what is happening on the task.

Workload/task saturation refers to the technician/inspector having too many different tasks to handle at the same time. A common outcome from task saturation is forgetting to do something.

Examples to look for:

1. *Physical health*

- Sensory acuity (e.g., vision loss, hearing loss, touch)
- Failure to wear corrective lenses
- Failure to use hearing aids or ear plugs
- Restricted field of vision due to protective eye equipment
- Pre-existing disease
- Personal injury
- Chronic pain limiting range of movement
- Nutritional factors (missed meals, poor diet)
- Adverse effects of medication
- Drug or alcohol use
- Complaints of frequent muscle/soft tissue injury
- Chronic joint pain in hands/arms/knees

2. *Fatigue*

- Lack of sleep
- Emotional stress (e.g., tension, anxiety, depression)
- Judgment errors
- Inadequate vigilance, attention span, alertness
- Inability to concentrate
- Slow reaction time
- Significant increase in work hours or change in conditions
- Excessive length of work day
- Excessive time spent on one task
- Chronic overloading
- Task saturation (e.g., inspecting rows of rivets)

3. Time pressure

- Constant fast-paced environment
- Multiple tasks to be performed by one person in a limited time
- Increase in workload without an increase in staff
- Too much emphasis on schedule without proper planning
- Perceived pressure to finish a task more quickly than needed in order to release the aircraft from the gate

4. Peer pressure

- Unwillingness to use written information because it is seen as a lack of technical skills/knowledge
- Lack of individual confidence
- Not questioning other's processes
- Not following safe operating procedures because others do not follow them

5. Complacency

- Hazardous attitudes (invulnerability, arrogance, over-confidence)
- Task repetition leads to loss of mental sharpness or efficiency

6. Body size/strength

- Abnormal reach, unusual fit, or unusual strength required for the task
- Inability to access confined spaces

7. Personal event

- Death of a family member
- Marital difficulties
- Change in health of a family member
- Change in work responsibilities/assignment
- Change in living conditions

8. Task distractions/interruptions

- Confusion or disorientation about where one is in a task
- Missed steps in a multi-step task
- Not completing a task
- Working environment is too dynamic

9. Memory lapse

- Forgot

10. Visual perception

- Misread dial/display because of parallax issues
- Misjudged distance
- Could not easily tell whether airplane was following marking into hangar because of visual angle

11. Lack of assertiveness

- Did not speak up and suggest a different solution
- Quickly gave up trying to get their position across

12. Stress

- Absenteeism
- Medical symptoms
- Technicians who get angry easily
- Unable to concentrate

13. Situation awareness

- Technician gets injured by passing vehicles
- Technicians tripping over cords or materials on the floor

14. *Work/task saturation*

- *Trying to carry out too many tasks at the same time*
- *Forgets to carry out one of the subtasks*

15. *Other*

- Absenteeism
- Vacations
- Medical leave
- Risk-taking behavior

G. Environment and Facilities

The working environment/facilities can contribute to system failure. For example, temperature extremes (either too hot or too cold), high noise levels, inadequate lighting (reflection/glare, etc.), unusual vibrations, and dirty work surfaces could all potentially lead to maintenance system failures. Concerns about health and safety issues could also contribute to maintenance technician system failures.

Examples to look for:

1. *High noise levels*

- High noise impacts the communication necessary to perform a task
- Extended exposure to noise reduces ability to concentrate and makes one tired
- Noise covers up system feedback during a test

2. *Hot*

- Work area is too hot so the task is carried out more quickly than usual to get back to an air conditioned room as quickly as possible
- Extremely high temperatures cause fatigue
- Long exposure to direct sunlight
- Exterior components or structure too hot for maintenance technicians to physically handle or work on

3. *Cold*

- Work area is too cold so the task is carried out quickly to get back to a heated room as quickly as possible
- Long exposure to low temperature decreases sense of touch and smell
- Technician has to wear gloves and heavy clothing, which could interfere with carrying out the task

4. *Humidity*

- High humidity creates moisture on aircraft, part and tool surfaces
- Humidity contributes to fatigue

5. *Rain*

- Causes obscured visibility
- Causes slippery or unsafe conditions

6. *Snow*

- Causes obscured visibility
- Causes slippery or unsafe conditions
- Protective gear makes grasping, movement difficult

7. *Lighting*

- Insufficient for reading instructions, placards, etc.
- Insufficient for visual inspections
- Excessive—creates glare, reflection, or eye spotting

8. *Wind*

- Interferes with ability to hear and communicate
- Moves stands and other equipment (creates instability)
- Blows debris into eyes, ears, nose or throat
- Makes using written material difficult

9. Vibrations

- Use of power tools fatigues hands and arms
- Makes standing on surfaces difficult
- Makes instrument reading difficult

10 Cleanliness

- Loss of footing/grip due to dirt, grease or fluids on parts/surfaces
- Clutter reduces available/usable work space
- Inhibits ability to perform visual inspection tasks

11. Hazardous/toxic substances

- Reduces sensory acuity (e.g., smell, vision)
- Exposure causes headaches, nausea, dizziness
- Exposure causes burning, itching, general pain
- Personal protective equipment limits motion or reach
- Exposure causes general or sudden fatigue
- Exposure causes general concern about long term effect on health

12. Power sources

- Not labeled with caution or warning
- Guarding devices missing or damaged
- Power left on inappropriately
- Circuit protection devices not utilized or damaged
- Cords chafed, split, or frayed

13. Inadequate ventilation

- Strong odor present
- Burning or itching eyes
- Shortness of breath
- Sudden fatigue

14. Markings

- White guide lines into hangar not painted
- White guide lines into hangar faded/chipped and hard to see
- Stop lines in hangar not painted or hard to see

15. Labels/placards/signage

- Bin labels for parts are faded and hard to read
- Placards needed for Minimum Equipment List (MEL) items are unavailable
- Warning signs regarding hazardous substances not posted
- Serviceable/unserviceable tags not hung on parts

16. Confined space

- Hard to enter
- Hard to move around
- Need watch person
- Need breathing equipment

17. Other

- Area(s) not organized efficiently (difficult to find parts, work cards, etc.)
- Area too crowded with maintenance technicians and/or other personnel

H. Organizational Factors

The organizational culture can have a great impact on maintenance system failure. Factors such as internal communication with support organizations, trust level between management and maintenance technicians, management goals and technician awareness and buy-in of those goals, union activities, and attitudes, morale, teamwork, etc., all affect productivity and quality of work. The amount of ownership the technician has of his/her work environment and the ability to change/improve processes and systems is of key importance to technician morale and self esteem, which in turn, affects the quality of task performance. This section is also the section to use when violations occur as a result of not following work processes or procedures.

Examples to look for:

1. *Quality of support from technical organizations*

- Inconsistent quality of support information
- Late or missing support information
- Poor or unrealistic maintenance plans
- Lack of feedback on change requests
- Reluctance to make technical decisions
- Frequent changes in company procedures and maintenance programs

2. *Company policies*

- Unfair or inconsistent application of company policies
- Standard policies do not exist or are not emphasized
- Standard error prevention strategies do not exist or are not applied
- Inflexibility in considering special circumstances
- Lack of ability to change or update policies

3. *Not enough staff*

- Not enough trained personnel
- Not enough trained personnel at the time

4. *Corporate change/restructuring*

- Layoffs are occurring
- Early retirement programs drain experience
- Reorganizations, consolidations and transfers cause more people to be in new jobs
- Demotions and pay cuts
- Frequent management changes

5. *Union action*

- Contract negotiations create distractions
- Historical management/labor relations are not good
- Positive or negative communication from union leadership
- Strike, work slowdown, or other labor action creates a disruption

6. *Work process/procedure*

If the work process or procedure is followed but is error inducing, then check this box. Reasons that this might occur include:

- Standard operating procedures (SOPs) incorrect
- General maintenance manuals outdated
- Inadequate inspection allowed
- Process/procedure does not obtain the desired outcome

7. *Work process/procedure not followed*

This box would be used for a violation of work processes or procedures that should have been followed, but were not followed. If this occurs, check this box. Then determine whether not following this process or procedure is a work group normal practice (norm). If it is, then check box 9 below.

- Skipped operational check
- Required protective equipment not used=
- Did not use "parts removed" tag

8 Work process/procedure not documented (e.g., use tribal knowledge)

The work process/procedure is a part of tribal knowledge, and not officially documented. People perform the process/procedure as how they learn from others in a group, instead of following a written standard.

- No procedure for radio check before towing operation
- No inspection criteria
- No procedure for proper use of safety equipment

9 Work group normal practice (norm)

If a technician has not followed a work process or procedure that he/she should have, it is very important to determine whether most other technicians do the same thing in this situation.

- Documented procedure — most people in the same situation do not follow the written process or procedure
- Undocumented procedure — most people in the same situation do the procedure without documenting it like the technician did.

10 Team building

- Management does not provide team building training to staff
- Management does not encourage staff to work on teams to solve process issues

11 Other

- Company is acquired by another company
- Work previously accomplished in-house is contracted out
- Overall inadequate staffing levels

I. Leadership/Supervision

Even though supervisors normally do not perform the tasks, they can still contribute to maintenance system failure by poor planning, prioritizing, and organizing of job tasks. Delegation of tasks is a very important supervisory skill and if not done properly, can result in poor work quality. Also, there is a direct link between the management/supervisory attitudes and expectations of the maintenance technician and the quality of the work that is performed.

Supervisors and higher-level management must also provide leadership. That is, they should have a vision of where the maintenance function should be headed and how it will get there. In addition, leadership is exhibited by management "walking the talk," that is, showing the same type of behavior expected of others.

Examples to look for:

1. Planning/organization of tasks

- Excessive downtime between tasks
- Not enough time between tasks
- Paperwork is disorganized
- Tasks are not in a logical sequence

2. Prioritization of work

- Technicians not told which tasks to carry out first
- Important or safety related tasks are scheduled last
- Fault isolation is not performed without checking the most likely causes first

3. Delegation/assignment of tasks

- Assigning the wrong person to carry out a task
- Inconsistency or lack of processes for delegating tasks
- Giving the same task to the same person consistently
- Wide variance in workload among maintenance technicians or departments

4. *Unrealistic attitude/expectations*

- Frequent dissatisfaction, anger, and arguments between a supervisor and a technician about how to do a task or how quickly a task should be finished
- Pressure on maintenance technicians to finish tasks sooner than possible or reasonable
- Berating individuals, especially in front of others
- Zero tolerance for errors
- No overall performance expectations of maintenance staff based on management vision

5. *Does not assure that approved process/procedure is followed*

- Supervisor sees that technician is not following a process or procedure (e.g., is not wearing personal protective equipment or is not using a calibrated wrench for a torque task)

6. *Amount of supervision*

- "Look over the shoulder" management style
- Frequent questioning of decisions made
- Failure to involve employees in decision-making

7. *Other*

- Meetings do not have purpose or agendas
- Supervisor does not have confidence in group's abilities
- Management does not "walk the talk" and thereby sets poor work standards for maintenance staff

J. Communication

Communication refers to the transfer of information (written, verbal, or non-verbal) within the maintenance organization. A breakdown in communication can prevent a maintenance technician from getting the correct information in a timely manner regarding a maintenance task.

Examples to look for:

1. *Between departments*

- Written communication incomplete or vague
- Information not routed to the correct groups
- Department responsibilities not clearly defined or communicated
- Personality conflicts create barriers to communication between departments
- Information not provided at all or not in time to use

2. *Between mechanics*

- Failure to communicate important information
- Misinterpretation of words, intent or tone of voice
- Language barriers
- Use of slang or unfamiliar terms
- Use of unfamiliar acronyms
- Failure to question actions when necessary
- Failure to offer ideas or process improvement proposals
- Personality differences

3. *Between shifts*

- Work turnover not accomplished or done poorly or quickly
- Inadequate record of work accomplished
- Processes not documented for all shifts to use
- Job boards or check-off lists not kept up to date

4. *Between maintenance crew and lead*

- Lead fails to communicate important information to crew
- Poor verbal turnover or job assignment at the beginning of a shift
- Unclear roles and responsibilities
- Lead does not provide feedback to crew on performance
- Crew fails to report problems and opportunities for improvement to lead person
- Communication tools (written, phones, radios, etc.) not used

5. *Between lead and management*

- Little or no communication exists
- Goals and plans not discussed regularly
- No feedback from management to lead on performance
- Lead does not report problems and opportunities for improvement to management
- Management fails to communicate important information to lead

6. *Between flight crew and maintenance*

- Late notification of defect
- Aircraft Communications Addressing and Reporting [System](#) (ACARS)/data downlink not used
- MEL/Dispatch Deviation Guide DDG interpretation problem
- Logbook write-up vague or unclear

7. *Other*

- Computer or network malfunctions lead to loss of information
- E-mail not used or ignored

TYPES OF STRATEGIES FOR PREVENTING MAINTENANCE SYSTEM FAILURES

There are four broad categories of strategies for preventing maintenance system failures:

Error Reduction/Error Elimination

The most often used, and most readily available, error prevention strategies are those that directly reduce or eliminate the contributing factors to the error. Examples include increasing lighting to improve inspection reliability and using Simplified English procedures to reduce the potential for mis-interpretation. These error prevention strategies try to improve task reliability by eliminating any adverse conditions that have increased the risk of maintenance error.

Error Capturing

Error capturing refers to tasks that are performed specifically to catch an error made during a maintenance task. Examples include a post-task inspection, an operational or functional test, or a verification step added to the end of a long procedure. Error capturing is different than error reduction because error capturing does not directly serve to reduce the "human error." For example, adding a leak check does little to reduce the probability of a mis-installed chip detector. It does, however, reduce the probability that an aircraft will be dispatched with a mis-installed chip detector. This is why most regulatory authorities require a subsequent inspection of any maintenance task that could endanger safe operation of the aircraft if performed improperly.

While error capturing is an important part of error management, new views point to a general over-confidence in the error capturing strategy to manage maintenance error. In theory, adding a post-task inspection will require two human errors to occur in order for a maintenance-induced discrepancy to make it onto a revenue flight. In recent years, however, there has been a growing view that the additional inspection to ensure the integrity of an installation will adversely impact the reliability of the basic task. That is, humans consciously or subconsciously relax when it is known that a subsequent task has been scheduled to "capture" any errors made during the primary task. It is not unusual to hear an airline manager say that the addition of an inspection did little to reduce the in-service experience of the error. For example, several major carriers are pulling inspections out of scheduled line-maintenance tasks, in the hopes of improving quality.

Error Tolerance

Error tolerance refers to the ability of a system to remain functional even after a maintenance error. The classic illustration of this is the 1983 Eastern Airlines loss of all three engines due to O rings not installed on the chip detectors. As a strategy to prevent the loss of multiple engines, most regulatory authorities granting ETOPS (extended twin operations) approval prohibit the application of the same maintenance task on both engines prior to the same flight. The theory is that even if a human error is made, it will be limited to only one engine. This was not the case in the Eastern loss of all three engines. One type of human error, the same incorrect application of a task applied to all three engines, nearly caused an aircraft to be lost.

Another example of building error tolerance into the maintenance operation is the scheduled maintenance program for damage tolerant structures (e.g., allowing multiple opportunities for catching a fatigue crack before it reaches critical length).

Error tolerance, as a prevention strategy, is often limited to areas outside the control of the first line investigator. However, it is important for the first line supervisor or interviewer to be aware of this type of prevention strategy, and consider error tolerance when it may be the best way to effectively deal with the error.

Audit Programs

Audit programs refer to an approach that does not directly address a specific contributing factor. An audit is a high-level analysis of the organization to see if there are any systemic conditions that may contribute to error.

MEDA RESULTS FORM

Maintenance Error Decision Aid (MEDA) Results Form

Section I—General Information

Reference #: _____ Airline: _____ Station of Maintenance System Failure: _____ Aircraft Type: _____ Engine Type: _____ Reg. #: _____ Fleet Number: _____ ATA #: _____ Aircraft Zone: _____ Ref. # of previous related event: _____	Interviewer's Name: _____ Interviewer's Telephone #: _____ Date of Investigation: ____/____/____ Date of Event: ____/____/____ Time of Event: __:__ am pm Shift of Failure: _____ Type of Maintenance (Mx) (circle one): 1. Line -- If Line, what type? _____ 2. Base --If Base, what type? _____ Date Changes Implemented: ____/____/____
---	---

Section II - Event

Please select the event (check all that apply)

1. Operations Process Event

- ☐ a. Flight Delay __ days __ hrs. __ min.
☐ b. Flight Cancellation
☐ c. Gate Return
☐ d. In-Flight Shut Down
☐ e. Air Turn-Back
- ☐ f. Diversion
☐ g. Smoke/fumes/odor event
☐ h. Other (explain below)
- () 2. Aircraft Damage Event**

() 3. Personal Injury Event

- () 4. Rework** (e.g., did not pass Ops check/inspection)

() 5. Airworthiness Control

() 6. Found during Maintenance

() 7. Found during Flight

() 8. Other Event (explain below)

Describe the incident/degradation/failure (e.g., could not pressurize) that caused the event.

Section III - Maintenance System Failure

Please select the maintenance system failure(s) that caused the event:

1. Installation Failure

- ☐ a. Equipment/part not installed
☐ b. Wrong equipment/part installed
☐ c. Wrong orientation
☐ d. Improper location
☐ e. Incomplete installation
☐ f. Extra parts installed
☐ g. Access not closed
☐ h. System/equipment not reactivated/deactivated
☐ i. Damaged on remove/replace
☐ j. Cross connection
☐ k. Mis-rigging (controls, doors, etc.)
☐ l. Consumable not used
☐ m. Wrong consumable used
☐ n. Unserviceable part installed
☐ o. Other (explain below)

4. Fault Isolation/Test/Inspection failure

- ☐ a. Did not detect fault
☐ b. Not found by fault isolation
☐ c. Not found by operational/ functional test
☐ d. Not found by task inspection
☐ e. Access not closed
☐ f. System/equipment not deactivated/reactivated
☐ g. Not found by part inspection
☐ h. Not found by visual inspection
☐ i. Technical log oversight
☐ j. Other (explain below)

7. Personal Injury

- ☐ a. Slip/trip/fall
☐ b. Caught in/on/between
☐ c. Struck by/against
☐ d. Hazard contacted (e.g., electricity, hot or cold surfaces, and sharp surfaces)
☐ e. Hazardous substance exposure (e.g., toxic or noxious substances)
☐ f. Hazardous thermal environment exposure (heat, cold, or humidity)
☐ g. Other (explain below)

8. Maintenance Control Failure

- ☐ a. Scheduled task omitted/late/incorrect
☐ b. MEL interpretation/application/removal
☐ c. CDL interpretation/application/removal
☐ d. Incorrectly deferred/controlled defect
☐ e. Airworthiness data interpretation
☐ f. Technical log oversight
☐ g. Airworthiness Directive overrun
☐ h. Modification control
☐ i. Configuration control
☐ j. Records control
☐ k. Component robbery control
☐ l. Mx information system (entry or update)
☐ m. Time expired part on board aircraft
☐ n. Tooling control
☐ o. Mx task not correctly documented
☐ p. Not authorized/qualified/certified to do task
☐ q. Other (explain below)

2. Servicing Failure

- ☐ a. Not enough fluid
☐ b. Too much fluid
☐ c. Wrong fluid type
☐ d. Required servicing not performed
☐ e. Access not closed
☐ f. System/equipment not deactivated/reactivated
☐ g. Other (explain below)

5. Foreign Object Damage/Debris

- ☐ a. Tooling/equipment left in aircraft/engine
☐ b. Debris on ramp
☐ c. Debris falling into open systems
☐ d. Other (explain below)

3. Repair Failure (e.g., component or structural repair)

- ☐ a. Incorrect
☐ b. Unapproved
☐ c. Incomplete
☐ d. Other (explain below)

6. Airplane/Equipment Damage

- ☐ a. Tools/equipment used improperly
☐ b. Defective tools/equipment used
☐ c. Struck by/against
☐ d. Pulled/pushed/drove into
☐ e. Fire/smoke
☐ f. Other (explain below)

() 9. Other (explain below)

Did the Maintenance System Failure "fly" on the aircraft? () Yes () No

Describe the specific maintenance failure (e.g., auto pressure controller installed in wrong location).

IV. Chronological Summary of the Event, Including How Some Contributing Factors Lead to Additional Contributing Factors

(Use additional pages, as necessary)

V. Summary of Recommendations

(Use additional pages, as necessary)

Section VI - Contributing Factors Checklist

A. Information (e.g., work cards, maintenance manuals, service bulletins, maintenance tips, non-routines, illustrated parts catalogs, etc.)

- N/A ☐
- | | | |
|--|---|--|
| ☐ 1. Not understandable | ☐ 4. Too much/conflicting information | ☐ 7. Information not used |
| ☐ 2. Unavailable/inaccessible | ☐ 5. Update process is too long/complicated | ☐ 8. Inadequate |
| ☐ 3. Incorrect | ☐ 6. Incorrectly modified manufacturer's MM/SB | ☐ 9. Uncontrolled |
| | | ☐ 10. Other (explain below) |

Describe specifically how the selected information factor(s) contributed to the system failure.

Recommendations to correct the Contributing Factors listed above.

B. Ground Support Equipment/Tools/Safety Equipment [Personal Protective Equipment (PPE) and Collective Protective Equipment (CPE)]

- N/A ☐
- | | | |
|--|--|--|
| ☐ 1. Unsafe | ☐ 6. Inappropriate for the task | ☐ 11. Not used |
| ☐ 2. Unreliable | ☐ 7. Cannot use in intended environment | ☐ 12. Incorrectly used |
| ☐ 3. Layout of controls or displays | ☐ 8. No instructions | ☐ 13. Inaccessible |
| ☐ 4. Out of calibration | ☐ 9. Too complicated | ☐ 14. Past expiration date |
| ☐ 5. Unavailable | ☐ 10. Incorrectly labeled/marked | ☐ 15. Other (explain below) |

Describe specifically how selected ground support equipment/tools/safety equipment factor(s) contributed to the system failure.

Recommendations to correct the Contributing Factors listed above.

C. Aircraft Design/Configuration/Parts/Equipment/Consumables

- N/A ☐
- | | | |
|--|---|--|
| ☐ 1. Complex | ☐ 5. Parts/equipment incorrectly labeled | ☐ 9. Not user friendly |
| ☐ 2. Inaccessible | ☐ 6. Inappropriate for the task | ☐ 10. Consumable unavailable |
| ☐ 3. Aircraft configuration variability | ☐ 7. Easy to install incorrectly | ☐ 11. Wrong consumable used |
| ☐ 4. Parts/equipment unavailable | ☐ 8. Not used | ☐ 12. Expired consumable used |
| | | ☐ 13. Other (explain below) |

Describe specifically how the selected aircraft design/configuration/parts/equipment/consumables factor(s) contributed to system failure.

Recommendations to correct the Contributing Factors listed above.

D. Job/TaskN/A ☐

- | | | |
|---|--|---|
| ☐ 1. Repetitive/monotonous | ☐ 3. New task or task change | ☐ 5. Other (explain below) |
| ☐ 2. Complex/confusing | ☐ 4. Different from other similar tasks | |

Describe specifically how the selected job/task factor(s) contributed to the system failure.

Recommendations to correct the Contributing Factors listed above.

E. Knowledge/SkillsN/A ☐

- | | | |
|--|--|---|
| ☐ 1. Technical skills | ☐ 4. Airline process knowledge | ☐ 7. Teamwork skills |
| ☐ 2. Task knowledge | ☐ 5. Aircraft system knowledge | ☐ 8. Computing skills |
| ☐ 3. Task planning | ☐ 6. English language proficiency | ☐ 9. Other (explain below) |

Describe specifically how the selected knowledge/skills factor(s) contributed to the system failure.

Recommendations to correct the Contributing Factors listed above.

F. Individual FactorsN/A ☐

- | | | |
|---|---|---|
| ☐ 1. Physical health (including hearing and sight) | ☐ 5. Complacency | ☐ 10. Visual perception |
| ☐ 2. Fatigue | ☐ 6. Body size/strength | ☐ 11. Lack of assertiveness |
| ☐ 3. Time pressure | ☐ 7. Personal event (e.g., family problem, car accident) | ☐ 12. Stress |
| ☐ 4. Peer pressure | ☐ 8. Task distractions/interruptions | ☐ 13. Situation awareness |
| | ☐ 9. Memory lapse (forgot) | ☐ 14. Workload/task saturation |
| | | ☐ 15. Other (explain below) |

Describe specifically how the selected individual factors contributed to the system failure.

Recommendations to correct the Contributing Factors listed above.

G. Environment/FacilitiesN/A ☐

- | | | | |
|---|--------------------------------------|--|--|
| ☐ 1. High noise levels | ☐ 5. Rain | ☐ 9. Vibrations | ☐ 13. Inadequate ventilation |
| ☐ 2. Hot | ☐ 6. Snow | ☐ 10. Cleanliness | ☐ 14. Markings |
| ☐ 3. Cold | ☐ 7. Wind | ☐ 11. Hazardous/toxic substance | ☐ 15. Labels/placards/signage |
| ☐ 4. Humidity | ☐ 8. Lighting | ☐ 12. Power sources | ☐ 16. Confined space |
| | | | ☐ 17. Other (explain below) |

Describe specifically how the selected environment/facilities factor(s) contributed to the system failure.

Recommendations to correct the Contributing Factors listed above.

H. Organizational FactorsN/A ☐

- | | | |
|---|---|--|
| ☐ 1. Quality of support from Technical Organizations (e.g., engineering, planning, technical pubs) | ☐ 4. Corporate change/restructuring | ☐ 8. Work process/procedure not documented (e.g., use tribal knowledge) |
| ☐ 2. Company policies | ☐ 5. Union action | ☐ 9. Work group normal practice (norm) |
| ☐ 3. Not enough staff | ☐ 6. Work process/procedure | ☐ 10. Team building |
| | ☐ 7. Work process/procedure not followed | ☐ 11. Other (explain below) |

Describe specifically how the selected organizational factor(s) contributed to the system failure.

Recommendations to correct the Contributing Factors listed above.

I. Leadership/SupervisionN/A ☐

- | | | |
|--|---|---|
| ☐ 1. Planning/organization of tasks | ☐ 4. Unrealistic attitude/expectations | ☐ 6. Amount of supervision |
| ☐ 2. Prioritization of work | ☐ 5. Does not assure that approved process/procedure is followed | ☐ 7. Other (explain below) |
| ☐ 3. Delegation/assignment of task | | |

Describe specifically how the selected leadership/supervision factor(s) contributed to the failure.

Recommendations to correct the Contributing Factors listed above.

J. Communication

- N/A** ☐ 1. Between departments ☐ 4. Between maintenance crew and lead ☐ 7. Other (explain below)
☐ 2. Between mechanics ☐ 5. Between lead and management
☐ 3. Between shifts ☐ 6. Between flight crew and maintenance

Describe specifically how the selected communication factor(s) contributed to the system failure.

Recommendations to correct the Contributing Factors listed above

APPENDIX J - OPERATOR SERVICE BULLETIN PROCESS

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

J.1 SCOPE

This appendix describes operator handling of Service Bulletins (SB), Service Letters (SL), All Operator letters (AOL), All Operator Telex (AOT), and communications of this type.

J.2 INTRODUCTION

Operators receive notifications from a variety of sources suggesting possible inspections, modifications, and other actions on the operator's fleet. These notifications normally come in the form of established communication documents from the airframe manufacturer, component vendors, A4A, FAA, industry organizations, etc.

The most common notifications are in the form of service bulletins, Notice of Proposed Rulemaking (NPRM), Airworthiness Directives (AD), service letters (which come with many names: SIL, AOL, AOT, SL, etc.) from the equipment manufacturers or the regulatory authority. The priority for review and disposition and implementation of these various documents varies greatly and depends on the type of documentation as well as the information communicated. For example, an airworthiness directive is obviously given immediate review and appropriate engineering/tracking action is taken, although implementation may be delayed for years. On the other hand, a service bulletin from a component vendor may receive immediate review and action based on operational considerations. And finally, many service bulletins are never acted on by the operator, based on the lack of benefits or criticality of the recommended actions.

An operator may or may not implement a service bulletin. This decision is based on factors such as safety impact, cost, operator's previous experience, fleet age, operator's approach to reliability, downtime requirements, and other considerations. Once an operator makes a decision to implement a service bulletin, or similar document, the implementation methodology may vary greatly depending on the operator's processes for accomplishing this type of work. In some cases, a very detailed engineering order may be written and distributed throughout the organization for implementation. In other cases, a simple notification to a vendor or to the operator's shops to accomplish the service bulletin may be the proper mode of communications. An operator may choose to implement a service bulletin for a number of reasons. These may include:

1. Regulatory requirement
2. Safety considerations
3. Standardization considerations
4. Reduced maintenance costs
5. Reduced spare parts costs
6. Reduced operational costs
7. Improved reliability

J.3 OPERATOR SERVICE BULLETIN PROCESS

Figure J1 depicts a generic operator service bulletin process. This process contains some of the best practices used by operators today and is described in the succeeding paragraphs.

After the Service Bulletin (SB) is received by an operator, it is typically logged into a database. This database is used to track the document and solution as it moves through the process. Additionally, this database may be used to log SBs that are not performed for archive purposes, if desired.

The SB is first evaluated to determine if the bulletin is applicable for the operator's fleet. If applicable, the service bulletin is then evaluated to determine if it should be implemented. If the bulletin is not applicable nor implemented, the bulletin is filed and the process is finished.

The SB is next evaluated as to its nature. If the SB is required by an AD, then the process proceeds to the implementation stage. If the SB is not required by an AD, then the question must be asked “Should we do this?” This question may be answered differently by different Operators. Some of the issues that should be addressed in answering this question include:

- Are there known safety issues if the SB is not accomplished?
- What is the OEM’s recommendation (Alert, Special Attention, etc.)?
- What is the Operator’s experience with this problem?
- What would be the cost/financial impact/benefit of performing the SB?
 - Aircraft/component standardization
 - Downtime/labor required
 - Program duration
 - Reliability/Maintainability impact
 - Spare parts impact
 - Operational Impact

All of these sub-questions should be evaluated to determine if the SB should be accomplished. The answers to these questions may affect the level of management at which the overall question “Should we do it?” is answered. It may be beneficial for the operator to communicate and coordinate with the manufacturers to ensure that the manufacturer’s safety related recommendations are fully understood.

If the decision is to not perform the SB, that decision should be documented with the appropriate justification provided. Specifically, the effects of not performing the SB should be addressed. The SB may then be filed for future reference.

After the determination has been made to perform the SB, the implementation phase can begin. The first part of this process is to decide if a deviation to the SB is desired. If a deviation is desired, it should meet the intent of the SB and have proper approval. The operator may wish to communicate their deviations to the manufacturers to ensure the safety intent of the original SB is met. In the case of ADs, the Alternate means of compliance (AMOC) procedure are described in 14 CFR and Appendix L.

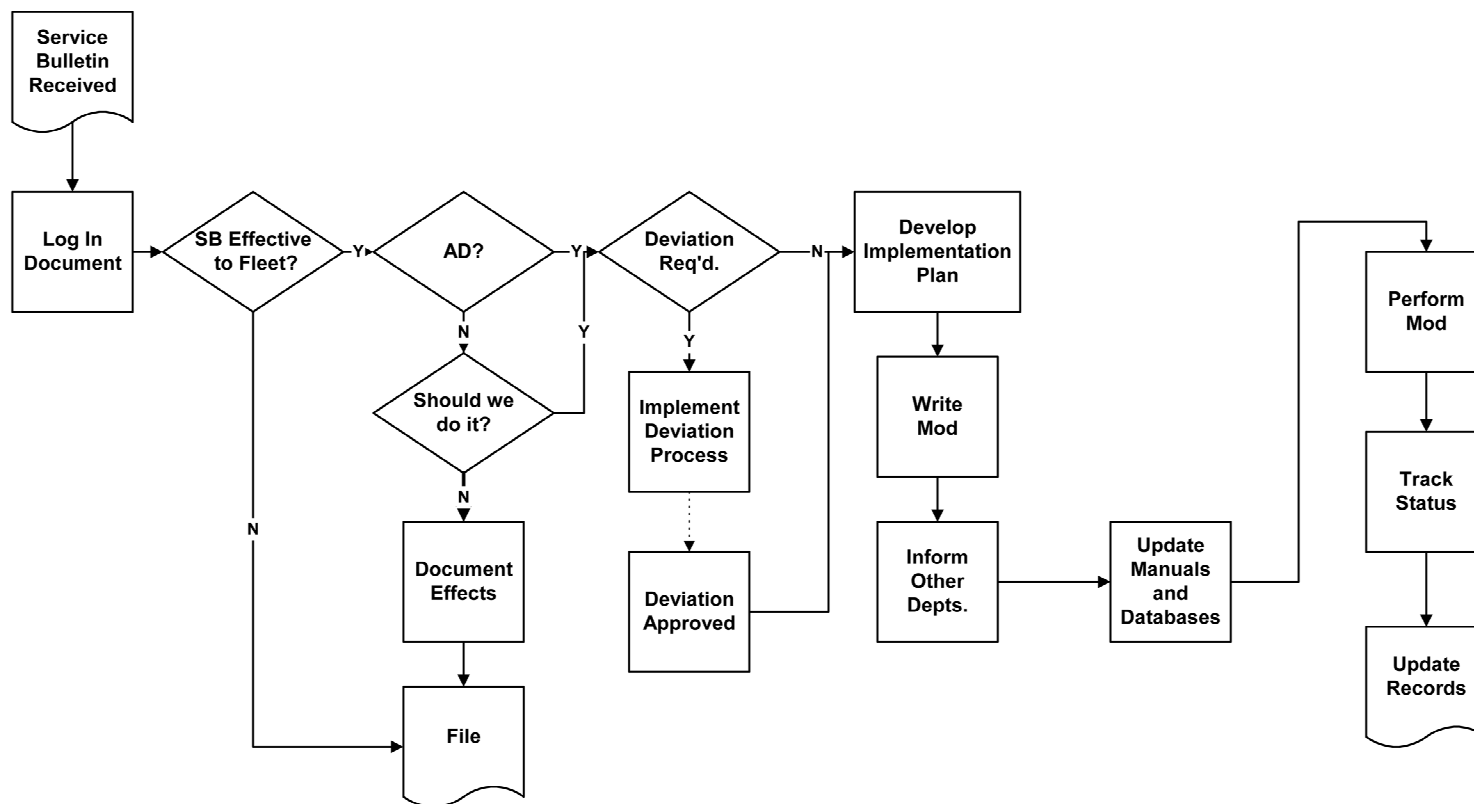


Figure J1 - Operator service bulletin process

The Operator must now develop a plan for implementation of the SB. This plan should involve all affected departments within the company. Some of the tasks and the issues that are usually involved in developing any plan are:

- Impact on safety?
- Method of retrofit? (How will the SB be performed?)
 - Internal shops
 - Outside vendor
 - Other configuration management impact
- Financial considerations and warranty implications
- Scheduling
 - Scheduled maintenance visit
 - Special visit
 - Manpower and skill availability
- Purchasing
 - Parts availability and lead time
 - Parts distribution

After the implementation has been planned, the Operator must prepare modification instructions per its internal procedures.

While the modification instructions are being written, other departments should review the draft modification documents and prepare to make necessary changes (manuals, databases, etc.) for SB compliance. Instructions for revising affected documents, including airframe maintenance, flight operations, maintenance planning document, and component maintenance manuals are normally included in the Operator's final modification instructions (Engineering Authorization, Engineering Order, etc.).

The elements of the implementation process should be monitored for accuracy and completeness. This is particularly important in addressing ADs, Manufacturer Required Changes or Operator Driven Changes. Special attention should be given to ensure against inadvertent de-modification.

Once the modification instructions are completed, the actual modification of the aircraft can begin. A prototype or mockup of the actual modification may be used to help identify unexpected problems or difficulties that may not have been addressed by the SB. This may be invaluable in cases of complex modifications. Many operators require that affected manuals are revised to reflect both pre and post modification configuration prior to physical modification of the aircraft. This practice ensures that airline personnel have accurate information to conduct ramp, maintenance and flight operations for all aircraft within the fleet type during the modification process. This also helps prevent de-modification of an aircraft SB during aircraft maintenance activities.

As the aircraft are being modified, the status of the fleet modification is tracked. After completion of the modification, the effectiveness of the modification in solving a problem may be monitored through normal monitoring processes described in this document. Although it is not always done, reporting SB status back to the issuer would confirm implementation and assist in evaluating its effectiveness. Depending on the operator's agreement with the SB issuer, reporting SB status back will allow the issuer to update applicable manuals to accurately reflect pre and post modification configuration by aircraft effectivity.

J.4 MODIFICATIONS OR ALTERATIONS (NON-SERVICE BULLETIN ORIGINATED)

Modifications or alterations to the airframe or its components by operators may be initiated based on safety, security, legal fitness or reliability and evaluated according to technical, operational or economic merit. A proposal may be made by any individual or group desiring a change. The engineering department responsible for aircraft configuration and control evaluates the feasibility and safety impacts of a proposal by providing the analysis and recommendation for a final decision. Additional information may be required such as material provisioning requirements and cost before the analysis can be completed. If the proposal is not approved, an explanation is provided and the request is closed. If the proposal is approved for incorporation into the fleet, action paperwork is initiated (e.g., Engineering Order, Engineering Authorization, Policy Sheet, Fleet Campaign Directive) and the proposal is passed on for planning, provisioning and incorporation. The operator may wish to communicate their modification or alteration to the manufacturers to ensure safety aspects are maintained.

Effective March 09, 2018, U.S. air carriers operating under 14 CFR part 121, in accordance with CFR Part 5 Subpart C - Safety Risk Management, will be required to apply safety risk management to the following conditions; Implementation of new systems, Revision of existing systems, Development of operational procedures, and Identification of hazards or ineffective risk controls through the safety assurance processes in subpart D of Part 5. This rule harmonizes U.S. requirements with International Civil Aviation Organization (ICAO) Annex 6, Part I standards. SBs generally comply with this requirement under the SB Issuer's SMS; however, operator-initiated changes may require analysis of the aforementioned systems to identify safety hazards and development of risk controls for those systems.

Refer to AC120-92B for additional information on SMS.

APPENDIX K - MANUFACTURER SERVICE BULLETIN PROCESS FOR SAFETY RELATED SERVICE INFORMATION

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

K.1 SCOPE

This appendix describes manufacturer's creation of safety related Service Information and, where appropriate, recommendations for Airworthiness Directives (ADs).

K.2 INTRODUCTION

Manufacturers create a variety of documents suggesting inspections, modifications, and other actions on the operator's fleet. These notifications normally come in the form of established communication documents from the airframe manufacturer. These notifications are most often in the form of a Service Bulletin (SB), or an update to the Maintenance Planning Document (MPD).

There exist several levels of SBs with respect to their significance relative to safety. The manufacturer's recommended priority for review, disposition and implementation of these varies depending on the type of documentation, as well as the information communicated. An operator may or may not choose to implement a service bulletin. They are not regulatory in nature, but some are issued in support of a corresponding AD, which is regulatory. Operator decisions regarding whether to incorporate a SB, and if so when, are based on factors such as safety impact, cost, operator's previous experience, fleet age, operator's approach to reliability, downtime requirements, regulatory requirements, and other considerations.

Non-safety related Service Bulletins constitute the majority of the bulletins. This appendix addresses only Service Bulletins related to enhancing safety, or issued in support of a corresponding AD intended to address a known unsafe condition.

Occasionally, the regulatory authority, in reviewing an issue, decides that it has enough safety significance (i.e., the issue represents an unsafe condition) to warrant mandatory action. Once a service bulletin becomes required by an AD, the operators must implement the bulletin within the specified timeframe.

In some cases, an unsafe condition addressed by an AD requires some periodic maintenance action to ensure that the condition does not exist or has not recurred. In these instances, the manufacturer may address these maintenance actions through an update of the Airworthiness Limitations section (ALS) to of Section 9 of the MPD. Unlike SBs that are not mandated by an AD, activities described in the ALS Section 9 of the MPD are mandatory and are required to be performed by regulation.

See Appendix M for further information on the AD process.

Advisory Circular 20-176A provides additional information for manufacturers on preparing service bulletins related to airworthiness directives.

K.3 KEY ASPECTS OF A SERVICE BULLETIN PROCESS

ATA Specification 111 and Specification 100 may be used as guidance in the development of a manufacturer's safety related SB processes.

K.3.1 Issue Evaluation

Each manufacturer should have a defined process for evaluating in-service events and determining whether (and if so, what) action should be taken.

K.3.2 Type Determination

Once the determination is made that the issue requires the issuance of service Information, a board/team needs to determine the type of information required (service bulletin type or MPD), and what actions need to be accomplished with the service information.

K.3.3 Processing

It can take several months to develop a service bulletin or MPD update. Because some safety issues may be so urgent that they require immediate mitigation, other more expedient means may be employed as interim solutions. Tools such as Service Letters, Maintenance Tips, All Operator Telexes (Messages, Wires) may be used to disseminate the information and/or interim actions to the operators while the service bulletin is being prepared.

K.3.4 Coordinating

For the case of an Alert Service Bulletin and some other safety related service bulletins, the regulatory authorities are notified. If the authorities determine that an issue should become an AD, they notify the manufacturer. Often, the manufacturer may coordinate with one or more of the affected operators in developing the service Information in order to ensure that it can be easily accomplished.

In certain cases, the regulatory authority initiates a request for service information based on their decision to issue an AD. In this case, the manufacturer complies by creating the required service information.

K.3.5 Releasing

Once the service information has been completed, it is released and distributed.

K.3.6 Monitoring

Manufacturers do not generally have the ability to monitor the implementation of service information by the operators. Some contractual arrangements do provide for monitoring of selected service bulletin implementation. Each operator determines whether or not a given bulletin should be implemented. The only required service actions are those directed by ADs, or those contained in the ALS.

APPENDIX L - AIRWORTHINESS DIRECTIVE DEVELOPMENT PROCESS

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the body of the document.

L.1 INTRODUCTION

Regulatory authorities are responsible for overseeing the continued operational safety of airplanes and engines. Included in this responsibility is issuing rules (e.g., Airworthiness Directives, or ADs) that require unsafe conditions be corrected. Unsafe conditions may result from design, manufacturing, operational or maintenance deficiencies.

Issuance of an AD, in accordance with 14 CFR 39 (in the U.S.; other nations have similar regulations), requires:

- a. That an unsafe condition exists in a product, part or appliance; and
- b. That the condition is likely to exist or develop in other products, parts or appliances of the same type design.

L.2 REGULATORY AUTHORITY ROLE (STATE OF DESIGN VERSUS STATE OF REGISTRY)

The role and responsibilities of a regulatory authority differs depending on whether it is acting as the State of Design (the State having jurisdiction over the organization responsible for the type design) or the State of Registry (the State where the airplanes are registered). These roles and responsibilities are defined in more detail in ICAO Annex 8.

For example, if the FAA is the State of Design for an airplane it suspects has an unsafe condition, it will confer with the airplane or engine Type Design Holder (TDH) to better understand the issue. If the FAA determines that an unsafe condition exists, it will coordinate with the TDH to obtain service information (e.g., a service bulletin) that will correct the unsafe condition. The FAA would then issue an AD that requires owners of U.S. registered airplanes accomplish the corrective action. The FAA would also issue a Mandatory Continuing Airworthiness Information (MCAI) that foreign States of Registry will review and take appropriate action for airplanes on their registry.

On the other hand, if a foreign regulatory authority (for example, EASA) issues an MCAI for an airplane for which they are the State of Design, the FAA, as the State of Registry, will review the MCAI. If the FAA agrees with the safety determination and corrective action it will issue an AD similar to the MCAI for which owners of U.S. registered airplanes must comply. The FAA typically has less involvement when acting solely as the State of Registry for a potential unsafe condition of a foreign airplane or engine, similar to the FAA having less involvement when acting as a validating authority to certify a foreign airplane or engine.

Similar relationships and roles exist between the other States of Design and States of Registry.

L.3 MAJOR STATES OF DESIGN

Currently there are six States of Design whose transport airplanes/engines are registered in the U.S. (similar relationships exist for other States of Registry). Each of these States of Design has a regulatory authority that issues ADs (or equivalent) and MCAIs. These authorities are the FAA (U.S.), EASA (European Union), ANAC (Brazil), TCCA (Canada), CAA (Israel), and the JCAB (Japan). The processes for determining if an unsafe condition exists, and for issuing ADs and MCAIs, differ from state to state, but all achieve the same goal.

L.4 FAA AD PROCESS

The development of ADs is a regulatory process and as such is subject to certain laws and Executive Orders. The following is a general description of the process to be followed in the development and issuance of ADs. Refer to the Airworthiness Directives Manual, FAA-IR-M-8040.1C, for more detailed information.

L.4.1 Decision to Start the AD Process

The decision to start the AD process is a key step. This decision is made by the FAA office that oversees the continued operational safety of the product.

The FAA office responsible for overseeing a product reviews data on in-service events, incidents, accidents, quality escapes (production and maintenance), engineering discoveries, safety recommendations and other sources to identify potential unsafe conditions for that product. More types of data are reviewed when the FAA is the State of Design Authority than when it is solely the State of Registry Authority (e.g., foreign type-design production quality escapes are typically not reviewed by the FAA). Additionally, for foreign State of Design products, the FAA reviews MCAIs in accordance with FAA order 8040.5 (Airworthiness Directive Process for Mandatory Continuing Airworthiness Information). This data review, and subsequent analysis, is done in accordance with FAA order 8110.107A (Monitor Safety/Analyze Data).

If the FAA is the State of Design Authority, then a quantitative risk analysis will typically be performed to assist in determining if an unsafe condition exists, and if so, how fast it needs to be corrected. For powerplant and APU issues, the Continued Airworthiness Assessment Methodologies (CAAM) is used (Advisory Circular 39-8). For other issues, the Transport Airplane Risk Assessment Method (TARAM) is used (PS-ANM-25-05). See appendix P for more information on these risk analysis methods. If the FAA is solely the State of Registry Authority responding to an MCAI the risk analysis step is bypassed (except in rare cases of unilateral action), as the FAA depends on the foreign authority to perform the risk analysis function. When it is the State of Design Authority the FAA initiating office will collaborate with the manufacturer of the affected product and obtain additional information about the potential unsafe condition.

If the FAA and the manufacturer disagree that an unsafe condition exists, the FAA will reconsider its position based on the results of the manufacturer's risk analysis. However, the FAA is the sole authority and makes the decision on whether to start the AD process, or once started, to discontinue it.

When the initiating FAA office signs the AD Worksheet, the AD process is considered to have legally started and additional restrictions on ex parte communication are levied (refer to the Airworthiness Directive Manual, FAA-IR-M-8040.1C, for additional information on ex parte communication). However, even then ex parte communications of needed factual information are not prohibited as long as the FAA documents all communications and records them in the rulemaking docket.

L.4.2 Determination of Corrective Action

Once the AD worksheet is signed, the FAA will contact the A4A in accordance with the Airworthiness Concern Coordination Process described in ATA Specification No. 111. This can allow time for air carriers to participate in the development of service instructions before they are proposed as an AD in the Federal Registry, e.g., by prototyping the proposed service instructions.

When the FAA is the State of Design Authority, it works closely with the manufacturer to define an acceptable corrective action; this could be completed either before or after the AD Worksheet has been signed. The FAA typically uses quantitative risk analysis results (either CAAM or TARAM, as appropriate) to assist in determining if a proposed corrective action plan is acceptable. If the ATA lead airline process is invoked the FAA will consider the feedback resulting from the lead airline evaluation of the proposed corrective actions.

When the FAA is solely the State of Registry, it is much less involved in the development of the corrective action. A corrective action has already been defined by the foreign State of Design Authority in the MCAI. The FAA typically adopts the MCAI corrective action as drafted (except for minor changes to the start of the compliance time).

L.4.3 Categories of ADs

Airworthiness Directives (ADs) are issued in several different ways, depending on the urgency of the unsafe condition. The three main methods of issuance, in increasing order of urgency, are:

- Notice of Proposed Rulemaking (NPRM) Followed by a Final Rule

After an unsafe condition is discovered, a proposed corrective action is published as an NPRM, which solicits public comment on the proposed action. After the comment period closes, the final rule is prepared, taking into account all the comments received, with the rule being changed as warranted by the comments.

- Immediately Adopted Rule (IAR) with Request for Comments

In certain cases, the urgency of an unsafe condition may warrant the immediate adoption of a rule without prior notice and solicitation of comments. This is an exception to the standard procedure, and should be used judiciously.

- Immediate Safety-of-Flight Rules (Emergency ADs)

When an unsafe condition exists that requires immediate action on the part of owners/operators, the AD may be issued directly to operators as a fax or by letter. Follow-up publication of one of these emergency ADs in the Federal Registry is normally issued as a final rule with request for comments.

NOTE: There are other types of ADs, such as Revisions, Corrections, Supplemental NPRMs, and Supersedures. Additionally, a no-notice final rule (with request for comments) may be issued when there are no aircraft currently on the U.S. Registry that are affected by the identified unsafe condition. In this case, a comment period is not necessary since there are no affected U.S. operators.

L.4.4 Responding to NPRM Comments

The initiating FAA office will consider all comments received concerning the NPRM. The proposed AD may be modified or withdrawn as a result of comment review. Comments received in response to the NPRM are discussed in the preamble to the rulemaking action.

When the FAA is the State of Registry Authority and receives an MCAI, it is typically adopted as drafted. It is in the interests of operators of foreign airplanes/engines to comment to the foreign State of Design Authority on ADs that the foreign authority has proposed before they become MCAIs, since once an MCAI is issued it is unlikely to be significantly changed by the FAA.

L.4.5 AD Issuance

Once the FAA has evaluated the NPRM comments, it typically follows with the issuance of the Final Rule after NPRM (FRAN). Because of their urgency, IARs and Emergency ADs are issued without a prior comment period.

When the FAA is the State of Design Authority, it will also issue an MCAI. Additionally, for all pending Emergency ADs, as well as certain other high-visibility ADs, the FAA will issue a Continued Airworthiness Notification to the International Community (CANIC). A CANIC is used to notify foreign civil airworthiness authorities of pending significant safety issues.

L.4.6 Follow-up Actions

The airlines are responsible for the implementation of the AD in accordance with the instructions included in the AD. Usually, these instructions will be contained in a manufacturer's service bulletin referenced in the AD. Implementing an AD in a large fleet requires a tremendous amount of planning.

Alternative Methods of Compliance (AMOC) to an AD may be proposed by an airline. The proposal may be for a different kind of corrective action or for a different schedule for compliance. AMOCs must keep the control program risk within the risk guidelines. The FAA office that issued the AD is responsible for approving AMOCs. Unlike ADs, AMOCs do not go through a public comment process before approval.

FAA inspectors are responsible for monitoring the airline incorporation of the AD. The airlines and the FAA inspectors should monitor the effectiveness of the AD in solving the safety problem and report deficiencies and problems.

L.5 EASA AD PROCESS

EASA ensures the continuing airworthiness of the products, parts and appliances it has certified (either through direct approval or after validation), by reacting without undue delay to a safety problem and issuing the applicable mandatory information. EASA issues ADs and MCAIs in accordance with their internal processes and procedures [Refer to "Continuing airworthiness of type design (CAP)" procedure and Annex I to ED Decision 2012/020/R (AMC and GM to Part 21)].

L.5.1 Decision to Start the AD Process

When EASA performs the functions and tasks of the State of Design Authority on behalf of EU Member States, the Project Certification Manager of the affected product, in coordination with teammates, reviews occurrences (to include in-service events, incidents, accidents, quality escapes [production and maintenance], engineering discoveries, safety recommendations and other sources) to identify potential unsafe conditions for that product. Then, based on risk analysis and investigations by the Design Approval Holder, or based on any other available information, the Project Certification Manager defines or agrees on appropriate actions.

The subsequent action may range from recommendation for improvements by the Design Approval Holder to corrective action (inspection, maintenance action or design change) that needs to be made mandatory by the issuance of an AD.

Annex I to ED Decision 2012/020/R (AMC and GM to Part 21) defines the criteria for determining an unsafe condition and the adequacy of the corrective action compliance times. The unsafe condition determination is largely qualitative, while the determination of the adequacy of the corrective action compliance times for hazardous and catastrophic failure conditions is quantitative.

When EASA performs the functions and tasks of the State of Registry on behalf of EU Member States, upon receipt of information that an AD has been issued by the State of Design Authority on an aircraft that is entered in the registry of one of the EU Member States, EASA either adopts that AD without any changes or issues its own AD based on the State of Design AD (refer to ED Decision 02/2003). In the case of adoption of a foreign AD without any changes, a simplified process applies as detailed in the process description on Adoption of Foreign State of Design AD.

L.5.2 Categories of ADs

- Proposed Airworthiness Directive (PAD) followed by a standard Airworthiness Directive (AD)

After an unsafe condition is discovered, a proposed corrective action is published as a PAD, which solicits public comment on the proposed action. After the comment period (usually 4 weeks) closes, the final AD is prepared, taking into account all the comments received, with the text possibly being changed as warranted by the comments.

- Final AD with Request for Comments (FAD)

In certain cases, the urgency of an unsafe condition or the length of the compliance time for the corrective action may warrant the immediate issuance of an AD without prior notice and solicitation of comments.

- Emergency AD (EAD)

When an unsafe condition exists that requires immediate action on the part of owners/operators, the AD may be issued as an EAD. The EAD does not change its status, unless in case of revision.

NOTE: There are also changes to existing ADs, such as Revisions, Corrections, Supersedures, and Cancellation Notices.

L.6 OTHER STATE OF DESIGN AUTHORITIES AD PROCESS

Other State of Design Authorities, ANAC (Brazil), TCCA (Canada), CAA (Israel), and the JCAB (Japan), also have processes to issue ADs (or equivalent) and MCAIs. Currently, these airworthiness authorities do not have defined quantitative risk analysis processes, so the determination of unsafe conditions and acceptable compliance times for the corrective action is largely qualitative.

APPENDIX M - HAZARD TRACKING

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

M.1 SCOPE

A major objective of safety assessment is to identify, prioritize and communicate risks associated with observed or anticipated problems effectively to management or other interested parties. This appendix provides examples of hazard tracking and hazard summary forms which help accomplish this objective.

Hazard Tracking is a safety management tool for controlling and maintaining the project safety records, providing:

- A “closed loop” system for identifying, recording, tracking and resolving all safety issues;
- Traceability to other safety records; and
- A summary of the safety activities performed.

M.2 HAZARD TRACKING

Hazard Tracking Forms and Hazard Tracking Summary Lists are two possible tools used in this document for the tracking of problems. Note that there are other ways of achieving the same objective.

The Hazard Tracking Form is a summary of the characteristics of a specific hazard being watched or worked. The Hazard Tracking Form should contain the following key elements:

- Problem description
- Event category
- Event hazard severity
- Event probability of occurrence
- Conditional probabilities of hazard level events given the observed event
- Size of the “at risk” population
- Current status (e.g., on hold awaiting resources, solution defined, implementation scheduled, implementation in process, implementation complete)
- Estimated time for completion of mitigation.
- Fleet risk exposure

This summary communicates the necessary key problem elements to management or other interested parties. Figure M1 presents an example Hazard Tracking Form containing these elements.

The Hazard Summary List identifies all open hazards, their risk levels and working status. This report gives visibility to the status of the multitude problems currently being tracked across any one product, but may provide little specific detail of the risk. The Hazard Tracking List can also be used to monitor cumulative risks. Figure M2 shows an example Hazard Tracking List. The risk levels should include a reference to appropriate regulatory criteria/guidelines.

PROBLEM DESCRIPTION	Uncontained engine disk fracture		PROBLEM NO.	1
CURRENT PRIORITY	1	PREVIOUS	None	
	PRIORITY LEVEL			
DATE IDENTIFIED	10/1/96	LAST REVISED	11/1/98	
CAUSE(S)	Engine rotor manufacturer advises potential casting flaw in 10 rotor disk S/N in fleet			
EVENT CATEGORY	1	EVENT HAZARD LEVEL	2	
EVENT	90% within	IMPACTED FAILURE	Uncontained	PROBABILITY 1000
Hr.; P=.9	CONDITION	engine disk		
	fracture			
PROBABILITY OF IMPACTED FAILURE CONDITION 1.7 E -07				
IMPACTED FLEET SIZE 10 rotor disk S/N in certain fleet				
UNCORRECTED RISK OF IMPACTED FAILURE CONDITION			1.7 E -07	
Assumptions: _____				

ACTION PLAN Replace engine disks before next revenue flight (ferry as necessary)				
STATUS (Interim Action)		Not applicable		
STATUS (Final Action)		8 changed out, 1 in shop, 1 in transit		
ASSISTANCE REQUIRED		Establish priority status in maintenance schedule		
RESPONSIBILITY		Operations		
CORRECTED RISK 1.0 E -09				
Assumptions: _____				

Figure M1 - Example hazard tracking form

OPEN HAZARDS				
CURRENT PRIORITY	PREVIOUS PRIORITY	HAZARD	STATUS	RESPONSIBILITY
1	None	Engine non-containment failure	IMPLEMENTING	Maintenance / Operations.
2	3	Autopilot Annunciation Failure	DEFINING FIX	Avionics
3	4	Speed brake failure	DEFINING FIX	Structures
4	5	Navigation display failure	HOLDING	Avionics
RETIRED HAZARDS				
	1	Primary Hydraulic failure	CLOSED	
	2	Fleet corrosion inspection	CLOSED	

Figure M2 - Example hazard summary list

APPENDIX N - LESSONS LEARNED

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the main body of the document.

N.1 INTRODUCTION

The NATO Lessons Learned (LL) Handbook from the *NATO, Joint Analysis and Lessons Learned Centre, 2016* provides the following broad definition for Lesson Learned: "The term *Lessons Learned* is broadly used to describe people, things and activities related to the act of learning from experience to achieve improvements. The idea of Lessons Learned in an organization is that through a formal approach to learning, individuals and the organization can reduce the risk of repeating mistakes and increase the chance that successes are repeated." More specifically, a LL is a compilation of knowledge gained by experience, observation or insight that includes a description of the situation that drove it, the outcome, and any pertinent recommendations that may improve future performance. The lesson learned may be positive or negative and may arise throughout a product or process lifecycle.

Modern organizations (companies, government agencies) have realized the importance of knowledge management (KM) as a powerful tool in ensuring their continued success. LL is an important facet of knowledge management as LL capture important knowledge key to product and continuous process improvements. The challenge facing any organization is to build a culture within which all feel comfortable and motivated to share their knowledge in a productive way.

Modern computing has enabled the creation and use of LL easily with the increasing availability of large scale databases, computing servers, internet connected devices, text mining, and the emergence of machine learning (artificial intelligence). LL are stored in databases that are easily accessed internal and external to the organization with sufficient information protection and security. Examples of such LL databases on the internet are the NASA Public LL System, FAA LL from Civil Aviation Accidents, Department of Energy (DOE) LL system.

There are many items learned during each day of airplane operations which are important to be recounted and carried forward for the aviation industry and individual companies to be successful. These LL are an existing, invaluable asset, which should be exploited in efforts to improve aviation safety.

N.2 OBJECTIVES

The purpose of a LL procedure is to learn efficiently from experience and to provide validated justifications for amending the existing way of doing things, in order to improve performance, both during the course of an operation and for subsequent operations. This requires lessons to be meaningful and for them to be brought to the attention of the appropriate authority able and responsible for dealing with them. It also requires the chain of command to have a clear understanding of how to prioritize lessons and how to staff them.

The objective of any LL process in the context of aviation safety is to provide a formalized and systematic approach of using experienced events to continuously improve safety and operational reliability of the in-service aircraft. This LL process should operate at all members and levels of the aviation industry. These lessons span from equipment experience to lessons of process improvement. The LL process also provides the key feedback communication paths from operator to OEM (aircraft or systems) so that in-service products and any future products may benefit from the in-use experience knowledge.

The introduction and implementation of a LL process in an organization enables a systematic accounting of experiences and solutions leading to the performance improvement including but not limited to:

1. Safety, accident prevention,
2. Reliability, availability, maintainability, cost,
3. Quality of products and processes,
4. Reduction of the number and cost of in-service product modifications,
5. Adaptation between human performance and machine performance and,
6. Adaptation to the customer needs.

It is important to note that the LL process described in this appendix is concerned with those events that have been identified as safety significant similar to the FAA LL but broader in scope. This is not intended to limit the users LL process scope but rather to focus the discussions and guidance of this appendix with the safety issues context.

N.3 GENERAL PRINCIPLES OF AN EFFICIENT SAFETY LESSONS LEARNED PROCESS

The NATO Lessons Learned Handbook identifies the following three basic steps to learning:

1. Identification: Collect learning from experiences.
2. Action: Take action to change existing ways of doing things based on the learning.
3. Institutionalization: Communicate the change (in a timely manner) so that relevant parts of the organization can benefit from the learning.

It also identifies common ways to learn from experience:

- LL Process: To gather, staff, action, and communicate lessons to ensure learning from experience is converted into actual improvement via a formal process.
- LL Information Sharing: To make use of databases, spreadsheets, websites, reports, or other media to store and communicate lessons.
- LL Community: To bring together Subject Matter Experts (SME) at working groups, training courses, conferences, and other events to share experience and learning.

An efficient LL process for safety embodies the following principles and inter-related steps:

1. Selection and prioritization of safety significant events,
2. Analysis of the prioritized events for generic causes and identification of the contributing factors,
3. Derivation of improvement recommendations,
4. Analysis of the effectiveness of improvement recommendations,
5. Effective implementation,
6. Systematic verification and monitoring effectiveness of the implementation, and adjustment as necessary, and
7. Systematic recording of the information generated by the above steps and traceability management.

Typically in an LL process, a standard data template is used to gather the candidate lesson which provides a consistent method to collect the data from a wide array of internal and external sources. Such templates may be part of a user interface tool which interacts with a central LL database in a LL system. Such systems allow for querying for previous lessons, their status, implementation results and effectiveness. In addition some systems have the subscriber capability where users can register their interest in specific product or process domain and the system keeps them abreast of the LL in their area of interest.

N.4 OPERATOR LESSONS LEARNED PROCESS

An operator LL process is intended to capture and communicate within the company lessons learned from operations and maintenance experiences. For example, the investigation of incidents and events is one of the most effective ways to identify past mistakes and capture the lessons learned from them. Important lessons learned can be documented, communicated, and incorporated into existing practices and programs. The lessons learned can also be used in the training process of operations and maintenance personnel.

N.5 MANUFACTURER LESSONS LEARNED PROCESS

It is important to emphasize the direct impact of the LL process on the improvement of safety. Using lessons learned during the product design phase can improve product safety by introducing:

- Consideration of new failure conditions/failure modes, or failure conditions/failure modes not traditionally considered in safety analyses,
- Better estimation of the consequences of failures (and better estimation of their associated risk level) when considering real situations with participation of human performance, operational and environmental conditions,
- Application of new safety methods and analyses processes to take into account new problems not traditionally covered (human errors, human/human interactions and behavior, human/machine interface, complex software/hardware network, etc.),
- Consideration of the evolution of the general environment and conditions in which the product is used: procedure changes, evolution of people culture, training, etc.

The results of a manufacturer LL process may be applied through equipment design standards or through company design guidelines, depending upon the importance of the lesson.

The design guidelines are used to refine design and operational policy for existing programs, and to define improved design and operational concepts for future programs. These guidelines or standards may address technical or organizational issues.

N.5.1 Manufacturer Lessons Learned Process Diagram

A generic Manufacturer LL process and the associated sub-processes and steps are shown in the following Figure N1.

N.5.2 Generic Manufacturer Lessons Learned Process Description

The Manufacturer Lessons Learned Process consists of three sub-process elements.

N.5.2.1 Sub-Process A: Event Selection and Recording

Sub-process A involves the selection/prioritization and recording from external and internal data sources of significant events (experience database). These sources are from product support, Continuous Airworthiness/Safety and Improvement monitoring processes, accident/incident databases, etc. The experience database can contain both successes and failures.

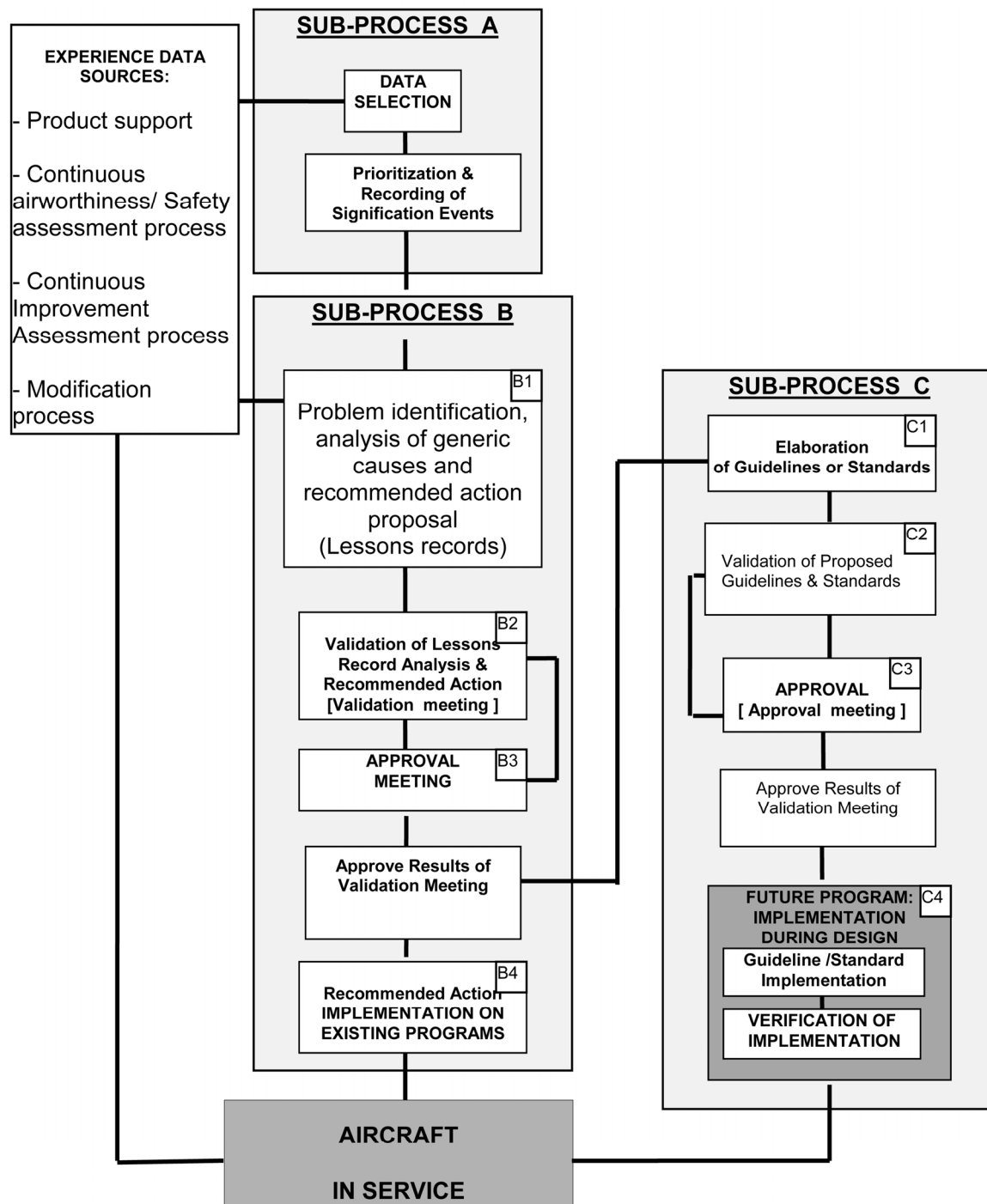


Figure N1 - Manufacturer lessons learned process

N.5.2.2 Sub-Process B: Events Analysis and Derivation of Recommended Actions

From the experience data base, significant events and cause records are selected based on problem subjects (design category, product category, concerned areas experienced) for analysis by specialists, and recommended actions are derived for improvement of in-service airplanes and current design programs.

Sub-process B consists of four steps:

Step B.1: Problem identification, analysis of generic causes, and recommended action proposal

This step involves selection from the experience database of significant information that will be analyzed. The selection is performed based on problem subjects: after identification of significant technical subjects (e.g., braking) and prioritization of the selected information, a technical record is prepared and sent to specialists involved for analysis of generic causes and proposal of recommended actions. These records and the study results are input items presented at validation meetings. The selected information is prioritized to provide visibility and priority of what is important to work on. This strategy allows users to focus on the top problems and to continually reduce the overall risk.

Step B.2: Validation meeting

The validation meeting starts with the technical records and a review of the recommended action proposals and specialist assessments on problems, generic causes and contributing factors. This is a multidisciplinary meeting that allows all specialists involved in the issue to analyze the concerned events and to review the proposal of recommended actions.

The validation meeting aims to:

1. Identify and validate the generic causes and contributing factors of the events (root causes which can be technical, methodological or organizational).
2. Develop or record developed intervention strategy prioritized to target these causes and contributing factors. These are the prioritized recommendations for improvements. This approach emphasizes those prevention or improvement recommendations that have the greatest impact.
3. Select and review the recommended action to improve the current program and prevent recurrence on a new design, new program, or modification of current programs. Review of recommended actions includes analysis of the effectiveness and feasibility of the recommended actions.

The recommended actions are:

1. Applicable to the existing products and programs,
2. Used to derive guidelines or design standards for new designs, new programs, or modifications on existing programs,
3. Used to derive new product specifications.

Results from validation meetings and associated recommended actions are recorded and stored in a database. Relationships with original events should be kept.

Step B.3: Approval meeting

Each recommended action is presented to an "approval committee." The objective of this committee is to approve the recommendation action(s) of the validation meeting.

The approval committee is composed of chief engineers responsible for current in-service programs. After approval, each chief engineer ensures implementation of the recommended action on the appropriate current in-service programs.

Recommended actions are also transmitted to sub-process C for development of guidelines or standards applicable to new design, new programs, or modifications on current programs.

Step B.4: Recommended Action implementation

This step describes the systematic and effective implementation of the recommended action.

Applicable recommended actions should be reviewed and monitored for verification of effectiveness and adjusted as necessary to ensure success.

N.5.2.3 Sub-Process C: Guideline or Standard Development, Implementation, and Verification Implementation

The focus of this sub process is to develop guidelines or standards applicable during the design phases of new products or modification phase of existing products.

Sub-process C consists of four steps:

Step C.1: Guideline or Standard development and recording

The main inputs for this step are the recommended actions generated from the validation meetings. Other inputs can also be used, including recommendations derived from analysis of events/causes described in technical publications or from information exchanges between companies, etc.

The guideline/standards development process can lead to either generation of new guidelines or improvements to existing guidelines. The guideline/standards are developed by committee and sent to specialists involved in the design process for review and comments.

The specialist's comments are then included in the final guideline/standard record.

Step C.2: Validation meeting

Guidelines and standards are technically validated during a validation meeting. Validation of guideline or standard includes analysis of the effectiveness and feasibility of the recommendation. Guidelines and standards can have technical and/or organizational impacts.

The validation meeting starts with the final guideline or standard record and reviews the proposals and its relation with the original recommended action. This is a multidisciplinary meeting, which allows all specialists involved in the issue to comment on the proposal, its means of application and its efficiency in accomplishing the original recommended action.

Step C.3: Guideline/Standard approval

As in Sub-process B, each guideline or standard has to be approved before implementation.

This step is conducted in the same way as in step B.3. The approval committee is composed of project managers and chief engineers of the responsible design department.

Step C.4: Implementation and verification of effectiveness (follow-up)

This step focuses on a systematic and effective implementation of the guideline or standard during the different phases of the new products design or modifications to existing products.

In case the guideline or standard is not fully implemented, justification and rationale should be recorded.

In order to be implemented, guidelines or standards are introduced in the applicable documents used during the design phase. If necessary, new documents may be generated.

Applicable guidelines or standards should be reviewed for effectiveness during product design reviews. All deviations and associated rationale should be approved during the reviews and recorded.

N.5.3 Evaluation of the Effectiveness of the Lessons Learned Process

Evaluation is accomplished through ongoing:

- Monitoring of deviations from recommended actions and guidelines or standards, and
- Monitoring for event reoccurrence during in-service operation.

APPENDIX O - FAA AND EASA QUANTITATIVE RISK ANALYSIS METHODS AND GUIDELINES

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the body of the document.

O.1 INTRODUCTION

This appendix provides an overview of some quantitative, statistical risk analysis methods that are used for assessing the risk of design related Continued Operational Safety (COS) issues in transport airplanes. The risk analysis results are used by the corresponding regulatory authorities during their COS issue safety deliberations. During these deliberations, the risk of a COS issue is compared to the acceptable risk guidelines to facilitate safety decision making and risk management. The risk analysis supports two crucial decisions: (1) is the COS issue being assessed an unsafe condition requiring mandatory corrective action, and (2) if so, is the proposed corrective action adequate (especially the compliance time)? An added benefit of performing a quantitative risk analysis is that the COS issue will be better understood qualitatively as well.

To produce a good risk analysis requires that the analyst be skilled in many topics, e.g., statistics, probability theory, the specific engineering discipline(s) of the discrepant system or component, how the discrepant system/component affects safety of flight. This appendix does not provide the detailed knowledge needed to perform a risk analysis, but rather an overview of the methods.

This appendix provides an overview of the FAA and EASA methods to be used when performing risk analysis of COS issues. See Appendix C for a discussion of general quantitative risk analysis methodologies.

O.2 RISK MEASURES AND RISK GUIDELINES

A COS issue is safe if its risk is acceptable (not zero, but rather, acceptable). There are two key elements to this definition of safety: (1) what is the risk of the COS issue, and (2) what is acceptable risk? The first is an objective, empirical based engineering exercise; the risk can be calculated using data and standard statistical/probabilistic formula and methods. The second is a subjective, societal value judgment.

There are several risk measures currently in use in the subject methods (many others are possible):

- Probability of Continued Airworthiness Assessment Methodologies (CAAM) level 3 (or higher) events per flight
- Probability of CAAM level 4 (or higher) events per flight
- Probability of hazardous failure per flight-hour
- Probability of catastrophic failure per flight-hour
- Probability of fatality per flight-hour
- Expected number of CAAM level 3 (or higher) events (risk factor)
- Expected number of CAAM level 4 (or higher) events (risk factor)
- Expected number of hazardous failures
- Expected number of catastrophic failures
- Expected number of fatalities
- Expected number of equivalent planeloads full of people fatally injured

Each of these risk measures has a corresponding acceptable risk guideline. There are unique guidelines for short-term acceptable risk and long-term acceptable risk, or uncorrected acceptable risk and control program acceptable risk, as applicable.

The risk guidelines are used to help in determining if a COS issue is an unsafe condition. A COS issue may have less risk than would warrant an unsafe condition determination, and not need mandatory corrective action, although there may be some safety benefit in taking action voluntarily. One vehicle that the FAA uses to alert operators of the opportunity to enhance safety through voluntary action is a Special Airworthiness Information Bulletin (SAIB).

O.3 DISCRETIONARY AUTHORITY

The regulatory authorities that use quantitative risk analysis do so to assist in safety management decision making. The results of a risk analysis do not bind the authority to find a COS issue to be safe or to be an unsafe condition, nor bind them to find that a control program is acceptable or unacceptable. Situations may arise where the authority needs to act contrary to the risk guidelines due to other factors. However, a goal is for the authorities to make decisions that are consistent with the risk guidelines as much as possible. A safety issue may represent a failure to meet a specific aviation regulation or intent of certification; in these circumstances, the regulatory authority may require mitigation while setting the compliance time as a function of the risk.

An important aspect of discretionary authority that applies to all unsafe condition corrective action plans/campaigns is that the risk guidelines are NOT to be used as targets for determining the compliance time; i.e., extending the compliance time to the maximum (or near it) allowed by the risk guideline. Once an unsafe condition has been determined, the risk should be mitigated as soon as is reasonable to do so, while simultaneously remaining below the risk guideline.

O.4 RISK ANALYSIS METHODS

This appendix reviews two FAA risk analysis methods, AC 39-8 and the Transport Airplane Risk Assessment Method (TARAM), and one EASA method, ANNEX I to ED Decision 2012/020/R. For the FAA, AC 39-8 is used to assess the risk of powerplant and APU installations, while TARAM is used to assess the risk of hazards not covered by AC 39-8. The EASA method covers both the powerplant and non-powerplant domains.

All three methods calculate the risk of the COS issue being assessed in two ways: (1) the probability that a particular outcome (e.g., CAAM level 4 or higher events) will occur per flight or per flight-hour (i.e., the rate of occurrence or the hazard function), and (2) the total number of statistically expected occurrences of a particular outcome in the affected fleet over some future time period.

When the risk measure is the rate of occurrence of a particular outcome, if the rate is a function of the component's age then the age at which the rate is assessed must be considered (e.g., an older airplane or an older fleet may have a higher rate than a younger one). When the risk measure is the expected number of some particular outcome over some future time period, the common time periods to assess are 20 years, the remaining life of the fleet or the time to complete the corrective action(s).

O.4.1 AC 39-8 Overview

Advisory Circular (AC) 39-8 describes the Continued Airworthiness Assessment Methodologies (CAAM). The method uses CAAM levels when assessing risk. CAAM level 5 events have catastrophic consequences, level 4 events have severe consequences and level 3 events have serious consequences. There are risk guidelines for CAAM levels 3 and 4, for both the expected number of CAAM level events (risk factor) and for the probability of CAAM level events per flight. Currently there are no published risk guidelines for CAAM level 5 events.

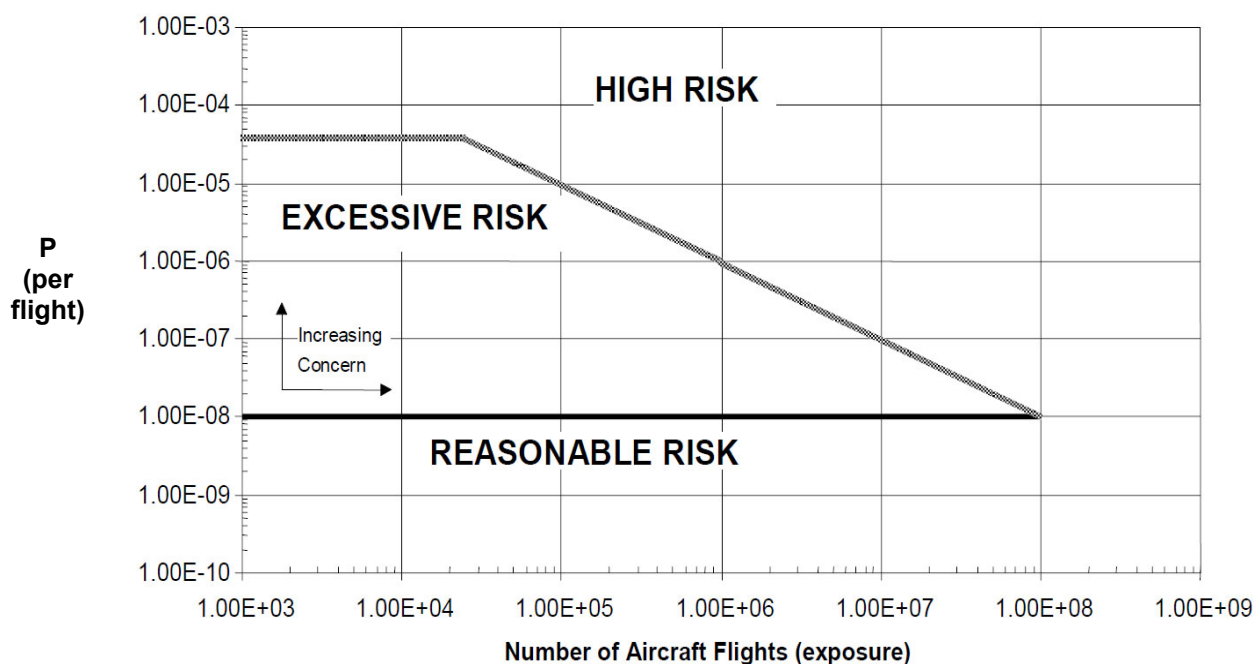
AC 39-8 provides conditional probabilities, termed Hazard Ratios in the AC, which are based on extensive historical accident/incident data. The Hazard Ratios are the conditional probability that given some event (e.g., an uncontained powerplant fire), a given CAAM level event or higher (e.g., CAAM level 3 or higher) occurs.

There are short-term and long-term risk guidelines. The short-term risk guidelines are used to judge the adequacy of the control program, while the long-term risk guidelines are used to assist in determining if a COS issue is an unsafe condition. The risk guidelines are shown in Table O1.

Table O1 - AC39-8 CAAM guidelines

	Level 3 Guidelines		Level 4 Guidelines	
	Risk factor	Per flight	Risk factor	Per flight
Long-term acceptable risk	N/A	1×10^{-8}	N/A	1×10^{-9}
Short-term acceptable risk	1.0	4×10^{-5}	0.1	4×10^{-6}

The risk guidelines are commonly presented in a trapezoidal plot, or “CAAM plot.” Figure O1 shows the CAAM plot for the CAAM level 3 guidelines (a similar plot is available for CAAM level 4 guidelines). The angled line in the trapezoid is where the risk factor is equal to its risk guideline of 1.

**Figure O1 - CAAM level 3 risk guidelines trapezoid**

There is a figure in AC 39-8 (AC 39-8 FIGURE 2) that shows event probability versus the event expectation for a Poisson process. FIGURE 2 in AC 39-8 is a linear-linear plot. That figure is reproduced here (as Figure O2).

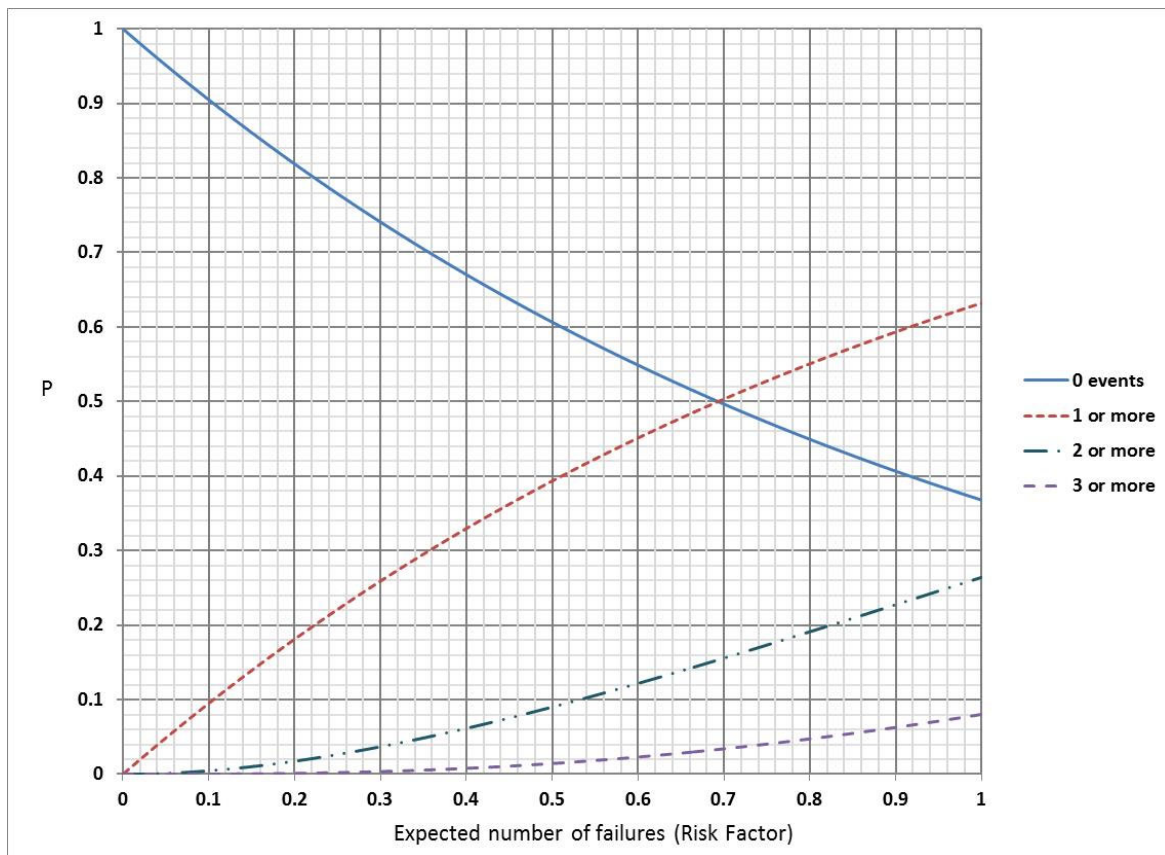


Figure O2 - Poisson distribution

The same function that is in Figure O2 can also be shown as a log-log plot; this is done in Figure O3. In risk analysis, thinking geometrically (log-log) may at times provide better insight than thinking arithmetically (linear-linear). The log-log plot also shows more detail in the low probability, low expectation region, which may be the region of interest (e.g., TARAM has a fleet risk guideline of 0.02).

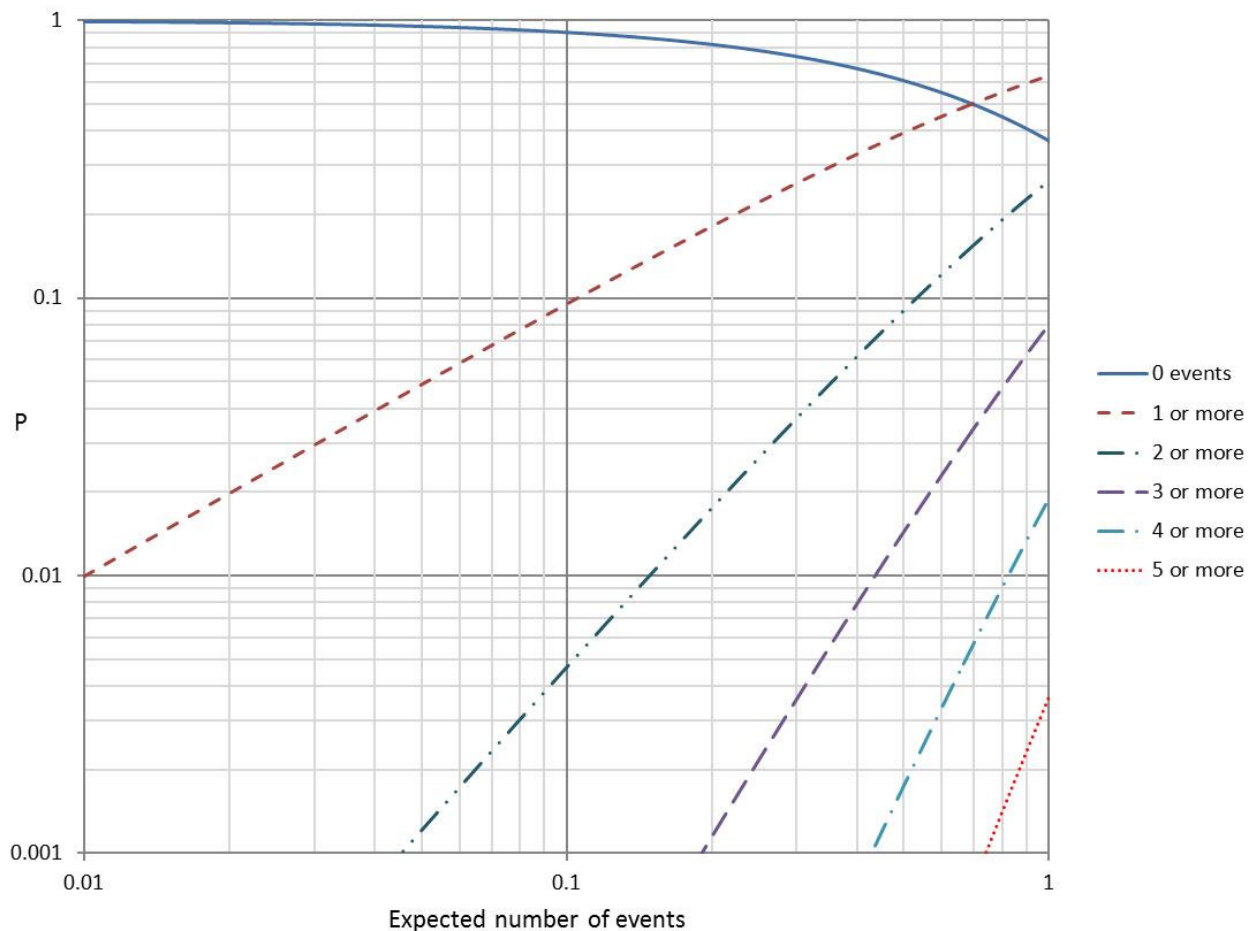


Figure O3 - Poisson distribution (log-log)

O.4.2 TARAM Overview

TARAM is described in FAA Policy Statement PS-ANM-25-05 and the TARAM Handbook. The risk measures used by TARAM are the probability of fatality per flight-hour, the expected number of fatalities, and the expected number of equivalent planeloads full of people fatally injured (i.e., the expected number of dangerous events multiplied by the Injury Ratio [IR]).

Similar to the work done for AC 39-8, the FAA determined values for certain conditional probabilities, which are termed Injury Ratios (IR), that are also based on extensive historical accident/incident data. An injury ratio is the single-event probability that those exposed to a condition or outcome, e.g., runway overrun, will suffer fatal injury.

Table O2 describes the various risk measures used in TARAM.

Table O2 - TARAM risk measures

Risk Value	Definition	Purpose
Total Uncorrected Fleet Risk	The number of weighted events statistically expected in the remaining life of the affected fleet if no corrective action is taken as a result of the identified potential unsafe condition. The events are weighted by the injury ratio (IR).	Provides a long-term forecast of future risk if no corrective action is taken. This helps determine whether an unsafe condition might exist and is used to guide the decision for corrective action.
Uncorrected Individual Risk	The highest probability per flight hour, expected to occur during a reasonable number of future flights, that an exposed individual will be fatally injured if no action is taken.	Used in cases where low fleet exposure or severity results in acceptable, total uncorrected fleet risk, as defined above, but the risk to individuals flying in high-risk airplanes is not acceptable. This risk calculation helps determine whether an unsafe condition may exist, and is used to guide the decision for corrective action.
90-Day Fleet Risk	The short-term average fleet risk in terms of fatalities within the affected fleet over the next 90 days if no corrective action is taken.	Provides a short-term risk forecast, and helps determine how urgently corrective action might be needed. The 90-day fleet-risk value provides management information for use in resource allocation.
Control-Program Fleet Risk	The risk within the affected fleet during the control program (the period when corrective action is being accomplished) in terms of fatalities.	Helps risk managers evaluate the acceptability of candidate corrective actions. Use the Risk Guideline in Table 3 to identify risk levels when more urgent action may be needed.
Control-Program Individual Risk	The highest probability per flight hour, expected to occur during a reasonable number of future flights, that an exposed individual will be fatally injured that is before corrective action is accomplished.	Used in cases where low fleet exposure or severity results in acceptable control-program fleet risk, as defined above, but the risk to individuals flying in those airplanes indicates that more aggressive action should be taken. It is used to guide the decision for the urgency of the corrective action.

Table O3 shows the allowable risk guideline for each of the risk measures that have an associated risk guideline (90 day fleet risk does not have an allowable risk guideline; it is primarily used as a consideration for which NPRM in the backlog to start drafting next).

Table O3 - TARAM risk guidelines

Safety Decision-Making		Priority	Risk Control Decision-Making		
Total Uncorrected Fleet Risk	Uncorrected Individual Risk	90-Day Fleet Risk	Control-program fleet Risk	Control-Program Individual Risk, Urgent Action May be Necessary	Control-Program Individual Risk, Not Airworthy
>.02 or .04	>10 ⁻⁷ /flight-hour	N/A	>3	>10 ⁻⁶ /flight-hour	>10 ⁻⁵ /flight-hour
Guidance: Use .02 guidance for transport-airplane types and fleets primarily used in commercial passenger operations. Use .04 for other types of operations.	Guidance: Use the uncorrected individual-risk-level guidance when risk variables, such as fleet size, fleet age, or exposed-occupant count, result in acceptable total uncorrected fleet risk, but the individual per-flight-hour risk is unacceptable.	Guidance: Use the 90-day fleet risk factor as a priority measure in comparison to other pending and envisioned corrective actions.	Guidance: Corrective action is required as soon as reasonably practical within the time period associated with the control-program fleet risk-level guidance. The risk-level guidance represents the maximum acceptable risk and is not to be used as a target value.	Guidance: Minimize, to the extent practicable, commercial-passenger service operations at individual risk levels above this level.	Guidance: Transport airplanes should not operate in commercial-passenger service above this level for any period of time.

Figure O4 shows some of the TARAM risk guidelines as a plot.

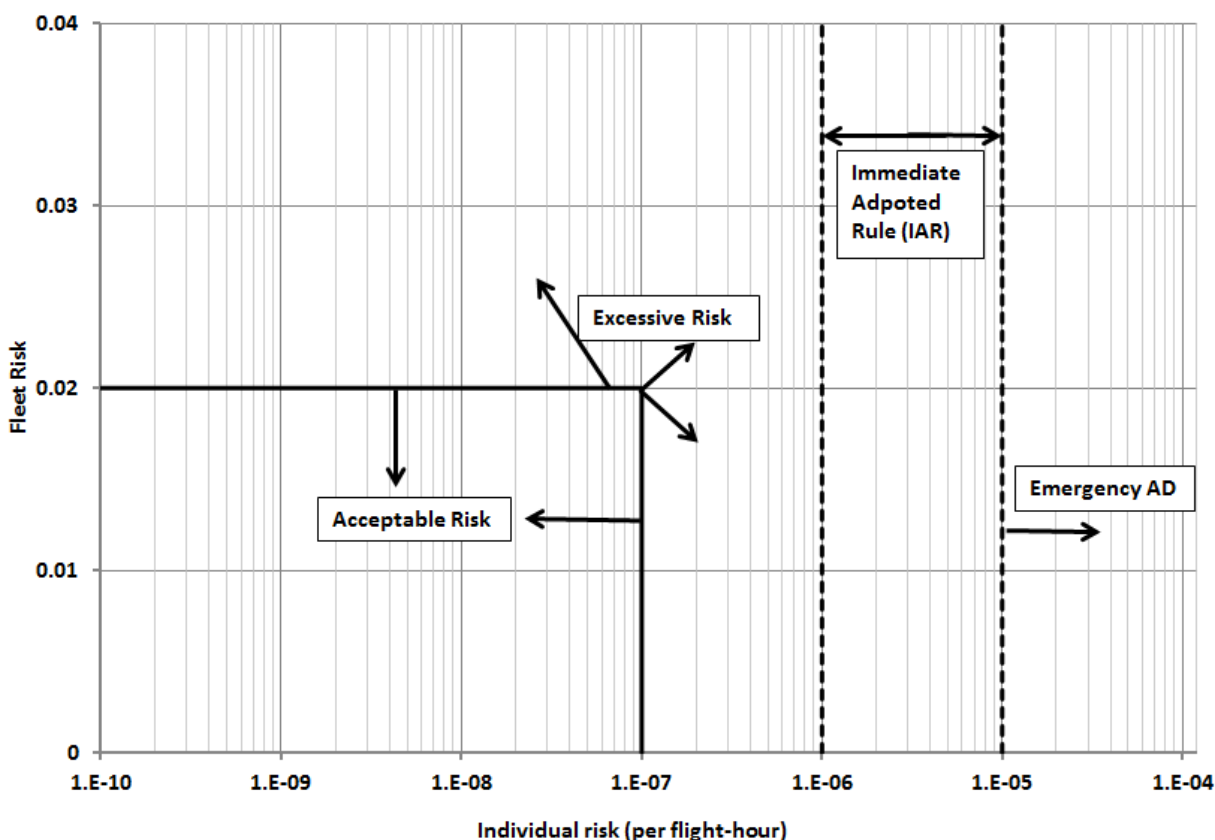


Figure O4 - TARAM risk guidelines plot

O.4.3 ANNEX I to ED Decision 2012/020/R Overview

The EASA method is described in ANNEX I to ED Decision 2012/020/R. The risk measures used by ANNEX I are the per flight-hour probability of catastrophic or hazardous failure conditions.

The determination of the adequacy of the corrective action compliance times for hazardous and catastrophic failure conditions uses quantitative risk analysis (corrective action programs are referred to as campaigns in the ANNEX). The unsafe condition determination is largely qualitative.

There are short-term and long-term risk guidelines. The short-term risk guidelines are used to judge the adequacy of the control program, while the long-term risk guidelines are used to assist in determining if a COS issue is an unsafe condition. The risk guidelines are shown in Table O4.

Table O4 - EASA long and short term acceptable risk criteria

	Hazardous Failure Conditions		Catastrophic Failure Conditions	
	Event level	Per flight-hour	Event level	Per flight-hour
Long-term acceptable risk	N/A	1×10^{-7}	N/A	1×10^{-9}
Short-term acceptable risk	0.5 max ⁵	2×10^{-4}	0.1 max ¹	2×10^{-6}

⁵ The event level allowable is a function of fleet size and airplane design life

The risk guidelines are commonly presented in a trapezoidal plot. Figure O5 shows the trapezoidal plot for a hazardous failure condition (a similar plot is available for catastrophic failure conditions).

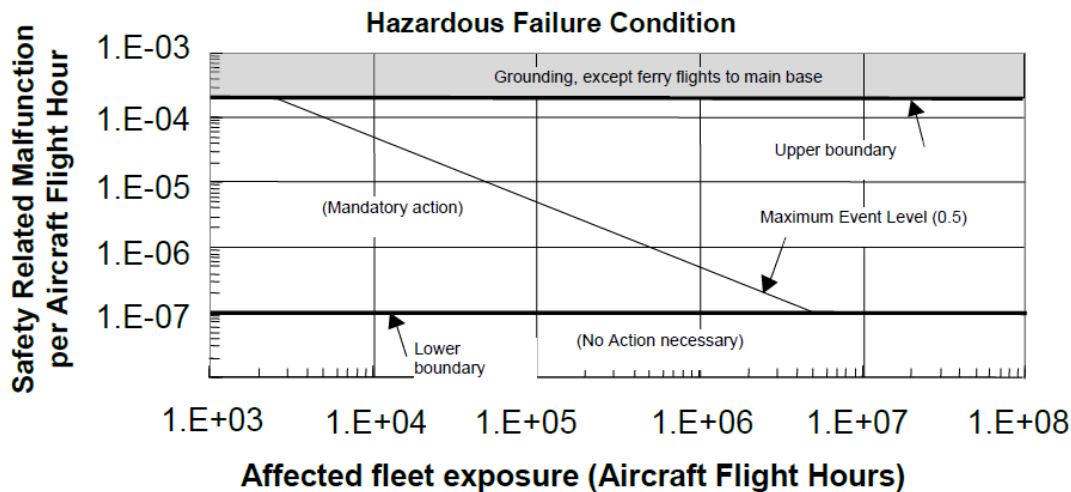


Figure O5 - EASA hazardous risk trapezoid

O.4.4 Differences between the Methods

TARAM and the ANNEX have guidelines expressed as probability per flight-hour while AC39-8 is expressed in probability per flight. In practice AC39-8 and ANNEX analyses may sometimes be performed either per flight or per flight-hour with no change in the applicable guideline.

Note that, for a two-hour flight, the ANNEX long-term catastrophic guideline is equivalent to AC39-8's level 4 guideline. The maximum event guideline of 0.1 for catastrophic and level 4 are also equivalent. Guidelines for the ANNEX hazardous and AC39-8's level 3 do vary. However, an ANNEX analysis may or may not take account of conditional probabilities of the hazardous or catastrophic event.

For catastrophic failure conditions the ANNEX guideline is 0.1 events while TARAM has a guideline of 0.02. TARAM explicitly requires that the analysis NOT use conservative assumptions while the ANNEX allows them. After taking into account the difference in assumptions used in the analysis, the apparent difference in the guidelines is largely rationalized.

For CAAM and TARAM the risk level and fleet expectation guideline is a constant, while in the ANNEX it is not a constant, but rather a function of fleet size and airplane design life.